

**Persistent threats and attacks combined with increasing regulatory and security policy compliance are compelling organizations to implement enterprise solutions for database activity monitoring, control and auditing.**

---

## BUSINESS NEED

Since databases contain some of the most business critical and sensitive information that organizations process, leading organizations are implementing database activity monitoring, security control and auditing solutions to implement the necessary security control.

- Many organizations deploy robust end point and perimeter security. However, these solutions typically lack the ability to detect many real-time threats to databases.
- Database technology has capabilities for auditing, but these features are frequently not implemented due to adverse impacts on system performance.
- Organizations have difficulty detecting the existence of sensitive or classified data contained in its databases which leaves the organization exposed to data breaches.
- Database administrators have powerful account privileges to administer data and database performance. As a result, these users can have access to sensitive data contained in the databases.
- Leading organizations have deployed enterprise security information and event management systems (SIEM) to consolidate and correlate this information to better detect threats and manage response. These organizations need security assessment, monitoring and auditing information to integrate with the enterprise solution.

---

## SOLUTION FEATURES

- Block privileged users from unauthorized access to sensitive database tables, without the risk of blocking legitimate access and while allowing privileged users - such as outsourced DBAs and developers - to continue performing routine administrative tasks such as backups.
- Prevent unauthorized changes to key systems, such as PeopleSoft, SAP and Oracle Financials, with closed-loop change control that leverages existing ticketing systems such as BMC Remedy.
- Perform database vulnerability assessments based on Department of Defense (DoD) standards such as the Database Security Technical Implementation Guide (STIG) and the Center for Internet Security (CIS) Benchmark.

- Mitigate the risk of web-based attacks with real-time identification of suspicious behavior and execute preventative actions.
- Provide enterprise database auditing and reporting to overcome limitations and performance impacts of native database auditing services.
- For Government agencies, simplify compliance with automated reports for NIST SP 800-53, OMB M-06-16, and Federal Information Security Management Act (FISMA).
- For businesses, automate and reduce cost of compliance with SAS70, the Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes-Oxley (SOX).
- Integrates with leading enterprise event and log management tools such as ArcSight, BMC and McAfee.

---

## VALUE

- Ensure privacy & integrity of critical data
  - Enforce change controls & access controls for critical systems
  - Across entire application & database infrastructure
  - Oracle, SQL Server, IBM DB2 & Informix, Sybase, MySQL, Teradata
  - SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects
- Increase operational efficiency
  - Automate & centralize internal controls
  - Across heterogeneous & distributed environments
  - Rapidly troubleshoot performance issues & application errors
  - Highly-scalable platform proven in most demanding data center environments worldwide
- No degradation of infrastructure or business processes
  - Non-invasive architecture
  - No changes required to applications or databases

---

## CONTACT

SECURE|IT

Phone: 703.464.7010

Email: [info@SecureIT.com](mailto:info@SecureIT.com)

Web: [www.SecureIT.com](http://www.SecureIT.com)