

## **Protect Databases from Security Threats and Automate Compliance**

**This paper describes the immediate needs confronted by Federal government agencies associated with protecting databases from security threats and attaining compliance with mission, security, privacy and financial regulations and policies.**

## Recent Security Breaches Involving Databases

The Federal Aviation Administration (FAA) had to warn over 45,000 employees that their personal data may have been compromised in a hack of one of its computer systems. The agency reported that one of its computers was illegally accessed and employee personal identity information was stolen electronically.

Heartland Payment Systems (HPY) in January 2009 disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants. Heartland officials stated that the intruders had access to Heartland's system for "longer than weeks" in late 2008. Heartland officials stated the breach may have affected over 100,000 individuals and has cost the company about \$12.6 million so far, including legal costs and fines from MasterCard and Visa.

At Monster.com, in January 2009, the company experienced the second breach of its employment search site Monster.com. The company lost a wealth of personal data belonging to millions of job seekers after its database was illegally accessed. The company warned all its customers that their names, birth dates, phone numbers, user IDs and passwords, email addresses, sex, and ethnicity may have been compromised. Monster.com strongly urged users to change their login credentials immediately and to be on the lookout for phishing emails.

## Challenges of Federal Agencies

### *Security Threats Continue to Mount and Increase in Sophistication*

Shawn Henry, the newly appointed Assistant Director of FBI's Cyber Division has warned that "a couple dozen" countries are eager to hack U.S. government, corporate and military networks. He withheld specific details of the countries in question but stated that cooperation with overseas law enforcements is of highest priority at FBI and that there has been great success fostering partnerships. However, Mr. Henry stated that certain countries have already mounted aggressive attacks against the U.S. particularly targeting websites under '.gov', '.mil', and '.com' top-level domains. "The threat that we face from organized groups that have infiltrated home computers, corporate computers, government computers [is] substantial and its impact on economy is a national security concern."

Organizations have worked to reduce vulnerabilities and adapted new technologies to detect and prevent security threats. However, attackers continue to create new and innovative ways to achieve their objectives. As a result, the threat landscape constantly shifts as the attackers identify weaknesses and exploit them through new more sophisticated techniques. Based on the data collected recently collected, analyzed and reported<sup>1</sup> by Symantec, we can observe that the current security threat landscape is predominantly characterized by the following:

---

<sup>1</sup> <http://www.symantec.com/business/theme.jsp?themeid=threatreport>

- Malicious activity has become Web-based
- Attackers targeting end users instead of computers
- Underground economy consolidates and matures
- Rapid adaptability of attackers and attack activity

"As cyber criminals move beyond mass-distribution style phishing scams, they are learning how to localize and personalize their attacks for better penetration," according to the Georgia Tech Information Security Center (GTISC) report<sup>2</sup>. Malware development expertise is rapidly maturing which provide the skills to exploit the continued weaknesses of poorly configured websites, applications and databases. As an example, the report described an exploit that sends a message from one person to another, about a YouTube video, including a link to the clip. The recipient clicks on the link, sees a prompt to download an updated version of Flash player to run the clip. When he clicks on the update, it actually installs malware on his computer.

Infections can occur even through legitimate Web sites as botnet delivery mechanisms are becoming more sophisticated. Users are unable to detect the threat and cannot deter it. Network managers can block known bad sites, but are unable to keep pace with the infections or cannot block access to a site for business reasons.

Another serious threat identified by GTISC is cyberwar. The report cites the evidence that implicates the Russian government in cyber attacks against Georgia. Cyber criminals are professional, organized and profit-driven, the report states. The report goes on to state that criminals now buy, lease, subscribe, or use a pay-as-you-go business model to obtain the latest in malware kits.

*Researchers at GTISC estimate that 15% of all online computers will become part of botnets thereby being infected with code that puts these computers under the control of the botnet.*

### **Applications and Databases Remain Vulnerable**

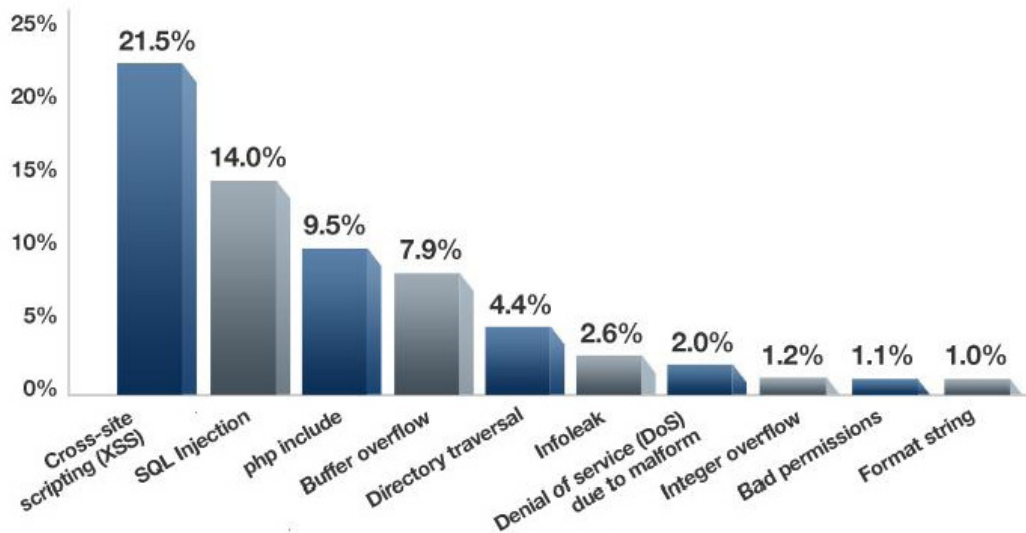
IBM's X-Force Lab reports<sup>3</sup> that Web-based vulnerabilities and threats continue to increase. They found that:

- Over the past few years, the focus of endpoint exploitation has dramatically shifted from the operating system to the Web browser and multimedia applications.
- Vulnerabilities affecting Web server applications are climbing and so are the attacks, both evidenced by newcomers to the most vulnerable vendor list and this year's automated SQL injection attacks.
- Although standard Web browsers are becoming more secure, attackers continue to rely on automated toolkits, obfuscation, and the prevalence of unpatched browsers and plug-ins to successfully gain hold of new endpoint victims.
- Although the most exploited Web browser vulnerabilities are one to two years old, the availability of public proof-of-concept and exploit code is speeding the integration of more contemporary exploits into toolkits.

<sup>2</sup> <http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf>

<sup>3</sup> <http://www-935.ibm.com/services/us/iss/xforce/midyearreport/>

- In the first half of 2008, 94 percent of public exploits affecting Web browser related vulnerabilities were released on the same day as the disclosure.



Courtesy of OWASP

IBM X-Force reports and Open Web Application Security Project<sup>4</sup> (OWASP) confirms that the predominate types of vulnerabilities affecting Web applications are cross-site scripting (XSS), SQL injection, and file include vulnerabilities. The graphic above charts each type of vulnerability. In the past few years, cross-site scripting has been the predominant type of Web application vulnerability, but the first half of 2008 saw a marked rise in SQL injection disclosures, more than doubling the number of vulnerabilities seen on average over the same time period in 2007. This increase explains the spike in the percentage of Web application disclosures attributed to SQL injection.

Forrester<sup>5</sup> reports through its analysis, that some of the top database security challenges are:

- DBAs are spending approx. 5% of their time on database security.
- 80% of organizations do not have a database security plan that addresses critical threats
- Only 20% of enterprises take advanced security measures —basic DBMS security alone is not good enough.
- Environment complexity makes it even more challenging —cloud computing, clusters, grids, replication, IaaS/SOA, Web 2.0, etc
- 60% of enterprises are behind in database security patches, making databases highly vulnerable.
- 75% of attacks are internal, which are harder to detect.

<sup>4</sup> <http://www.owasp.org>

<sup>5</sup> The Forrester Wave™: Database Auditing And Real-Time Protection, Q4 2007

***Security Policy and Regulations Continue to Mount with Increased Detail Required to Demonstrate Compliance***

Database Security Configuration Compliance

FISMA and associated OMB guidance requires agencies to ensure their computer systems conform to security configuration baselines published by NIST and DISA. Agencies must determine the relevant baseline, assess compliance to the standard, and manage change/remediation to eliminate non-compliance and associated risks. OMB requires agency CIOs to report on inventory count and progress on attaining and sustaining configuration compliance. This performance counts towards the agencies FISMA score and is audited by Office of Inspector Generals (OIG).

Data Inventory and Categorization and Protection of PII and Sensitive Information

The Office of Management and Budget issued memo [M-06-16 “Protection of Sensitive Agency Information”](#) which provided additional guidance to agencies regarding protection of Personally Identifiable Information (PII). This memo required all federal agencies to:

- Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive. This spans PDAs, laptops, USB storage devices, and backup media;
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

*NIST recently published a [Frequently Asked Questions \(FAQ\) for Sensitive Data Extracts](#)<sup>1</sup>. In this FAQ NIST answers common questions regarding OMB Memo 06-16. It provides guidance on the data which must be audited, the information that needs to be contained in the audit log, and provides approved methods for verifying that extracted data is either still required or has been deleted.*

OMB Memo 06-16 requires agencies to identify all personally identifiable information (PII) and agency sensitive information. Once inventoried, agencies must determine if the appropriate security controls are implemented, effective and continuously monitored.

Control Testing

Federal security policy requires all systems to be certified and accredited (C&A). NIST has defined standards for C&A. NIST Special Publication 800-53 defines the security controls for Low, Moderate and High systems. There are over 160 security controls defined that span the following areas:

FAMILY	CLASS
Access Control	Technical
Awareness and Training	Operational
Audit and Accountability	Technical

FAMILY	CLASS
Certification, Accreditation, and Security Assessments	Management
Configuration Management	Operational
Contingency Planning	Operational
Identification and Authentication	Technical
Incident Response	Operational
Maintenance	Operational
Media Protection	Operational
Physical and Environmental Protection	Operational
Planning	Management
Personnel Security	Operational
Risk Assessment	Management
System and Services Acquisition	Management
System and Communications Protection	Technical
System and Information Integrity	Operational

NIST SP 800-53A is now required as the standard for testing of controls. This standard defines the assessment cases required for each of the 160+ security controls. Organizations that do not organize to optimize control implementation and assessment efforts will face major increases in costs to annually maintain the C&A of its systems. NIST SP 800-37 also requires controls to be assessed at least annually (more frequently for HIGH systems). Therefore, automation to the greatest extent possible combined with making sure an organization and leverage all testing and assessment efforts performed throughout the year by different parts of the organization will help to drive down costs, reduce security risks, and increase compliance.

### ***Need to Adopt Emerging Technologies such as Cloud Computing***

Federal agencies, not unlike corporations, look to emerging technology to improve operations and reduce costs. Cloud Computing offers many benefits to Federal government agencies in these areas. However, there are many questions which involve data security which these organizations must seek answers and solutions from the cloud computing solution provider. GSA<sup>6</sup> recently released a Request for Information (RFI) seeking information from potential cloud computing vendors with questions regarding security practices and capabilities:

1. How is data handled and isolated?
2. How is data discovered within your information systems?
3. Can the provider guarantee that data will remain within the continental United States, both in transit and at rest? If so, how?
4. What are the roles and responsibilities regarding data ownership, e.g. logging data.
5. How will your company get customer's data back in-house either on demand or in case of contract termination for any reason?

<sup>6</sup> The GSA Office of the Chief Information Officer (OCIO), in concert with the IT Infrastructure Line of Business (ITI LoB)

6. How will your company handle data remnants throughout their service lifecycle?
7. What is your approach to addressing IT security challenges in cloud computing, in particular - dealing with hacker attacks, the potential for unauthorized access, and inappropriate use of proprietary data and IT applications. What are your processes and solutions for preventing these challenges from occurring?
8. Describe how your service offering could enable eDiscovery, forensic analysis, auditability, and other similar governance requirements.
9. What kind of intrusion detection and intrusion prevention systems do you use, and are your customers provided access to these?

## Critical Needs and Use Cases

To address this array of challenges and requirements, Federal government agencies must implement enterprise-wide database security solutions that:

- Provide real-time monitoring to respond to unauthorized or malicious activity for Oracle, Microsoft SQL Server, MySQL and IBM DB2 -- without impacting performance or requiring database changes combating external threats such as SQL injection.
- Restrict access to Personally Identifiable Information (PII) and other sensitive data by privileged users through identification of sensitive data, tables and records and implementation of real-time controls that restrict access.
- Capture database audit logs across all databases without impacting system performance and provide a means to alert based on events in the logs.
- Enforce separation of duties on database administrators for NIST 800-53 and DOD 8500 compliance by monitoring activity and generating NIST-specific reports for audits.
- Detect, monitor internal and external connections to enterprise database systems using both policy-based controls and anomaly detection to prevent unauthorized access and disruption by potential hackers as well as detection and blocking of insider attacks.
- Assess, measure and manage database security vulnerabilities and configuration compliance with standards from NIST, DISA and CIS.
- Automate a number of security controls associated with databases in NIST SP 800-53 and DOD 8500 to support certification and accreditation (C&A) and continuously monitor these controls to ensure effective implementation.
- Monitor access to sensitive or classified information by establishing thresholds and alerting if an application or user requests records over the threshold. This can indicate a SQL injection or some similar attack and prevent further access from the application or user.

- Control service accounts so that they only access the database from a defined source IP addresses (authorized internal addresses, authorized external addresses), and that these service accounts only run a defined, narrow set of authorized queries.
- Implement OMB 06-16, Privacy Act and HIPAA compliance, identify sensitive data and implement controls which restrict access, log activity and extracts, and alert on suspicious activity.
- Track and manage changes with closed-loop integration with external change management tools to ensure database changes are tracked and approved prior to implementation.

## SecureIT Database Security Solution

The team of SecureIT and Guardium understand the security challenges of Federal Government agencies and the threats against databases. Together, the team offers a database security, monitoring and auditing solution that can ensure the integrity of business critical and sensitive information and prevent information leaks from the data center. SecureIT understands and has experience implementing enterprise security programs to address security threats and compliance with FISMA, FISCAM, Privacy Act, HIPAA, and other regulations and policies. The Guardium7 enterprise security platform prevents unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise databases, custom applications and commercial products including Oracle EBS, PeopleSoft, SAP, and Business Intelligence. The team of SecureIT and Guardium can provide a solution that automates security operations and optimizes operational efficiency with a scalable, multi-tier architecture that centralizes compliance controls across your entire application and database infrastructure.

### *Summary of Benefits and Features*

The SecureIT Guardium 7 solution provides the essential tools needed by Federal Government Database Administrators (DBA), Chief Information Security Officers (CISO), Information Owners (IO) and Chief Privacy Officers (CPO) to protect against the constantly-increasing number of security threats. The solution provides a wide range of security features that address critical use cases such as audit database usage, enforce policies to prevent unauthorized access, controls and reporting for security and data privacy regulations and compliance. A summary of these benefits and features are:

- Data discovery and classification tools to identify sensitive or classified data and prevent leakage;
- Vulnerability assessment solution to identify and resolve database application vulnerabilities;
- Implement controls to restrict access to sensitive data;
- Track sensitive data extractions (OMB 06-16);

- Real-time database activity monitoring to proactively identify unauthorized or suspicious activities with the ability to take proactive measures;
- Correlation alerts to notify the proper personnel on events such as an unusual number of SQL errors or login failures;
- Baselineing to get a clear picture of normal database usage to develop policy rules based on and alerts for activity considered abnormal;
- Enterprise wide auditing and compliance solution for databases to simplify FISMA, FISCAM, Privacy Act, OMB, NIST, DIACAP, and HIPAA policy requirements;
- Change control solution to prevent unauthorized changes to database structures, data values, privileges, and configurations; and
- Continuous monitoring of database-related security controls to support Certification and Accreditation (C&A) per NIST SP 800-53A and NIST SP 800-37

**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

**Solutions for Federal Government Agency Database Security Challenges**

Federal Government Requirement	SecureIT Guardium Solution Summary
Identifying systems and databases	Using Guardium’s auto-discovery capability performs a network discovery of the database environment; SecureIT can create a visual access map showing all interactions among database servers, tables, clients, and applications. This helps quickly identify authorized and unauthorized users, applications, database servers, etc. Database auto-discovery can also be scheduled to execute on a regular basis, in order to prevent the introduction of rogue servers and ensure that no critical information is “forgotten.”
Understanding the data stored in databases	Using a list of databases mapped out by the auto-discovery process, SecureIT uses Guardium’s Classifier module to automatically discover and classify sensitive data inside databases. The Classifier uses an

Federal Government Requirement	SecureIT Guardium Solution Summary
	<p>intelligent database crawler to efficiently search for customizable patterns such as 16-digit credit card numbers and 9-digit Social Security numbers (based on regular expressions).</p> <p>If the client wishes to scan repositories outside of databases, SecureIT uses other tools to discover, categorize and manage remediation.</p>
<p>Ability to detect and audit network connections</p>	<p>Using Guardium’s real-time monitoring technology SecureIT can use both policy-based controls and anomaly detection to prevent unauthorized activities by potential hackers, privileged insiders, and end-users of enterprise applications. The solution continuously tracks all DBMS traffic at the network level and on database servers themselves. A visual access map allows you to quickly identify unauthorized users and applications with a graphical representation of all database servers, clients, subnets, and applications. Interactive drill-downs enable quick understanding of the “who, what, when, where, and how” of all database transactions.</p>
<p>Identify, control and monitor user accounts and privileged users</p>	<p>SecureIT can implement a solution to 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.</p>
<p>Compliance with mandated security configurations</p>	<p>SecureIT can assess and monitor databases for compliance with mandated security configurations such as DISA, NIST and CIS. The solution enables real-time compliance monitoring, and automatic enforcement of policy on an enterprise level. SecureIT can complement database security configuration assessment and monitoring with a solution for infrastructure and a means to manage and report on this information at the enterprise level.</p>
<p>Implement access controls for computer systems</p>	<p>The SecureIT Guardium solution contains advanced tools to provide a means to tailor ‘privacy sets’ or sensitive data elements in order to determine, establish and then implement access controls on databases. The solution can then identify suspicious activity. For example, Social Security Numbers and bank accounts can be tagged to block access for non-routine transactions, unauthorized applications or privileged users.</p>
<p>Gather and use audit data to detect computer intrusions and misuse and support incident investigation</p>	<p>The SecureIT Guardium solution can be implemented to provide enterprise-wide database auditing and reporting. The solution overcomes limitations and performance impacts of native database auditing services. This complete audit trail of database activity allows compliance with notification laws should a compromise occur and provide information to assist in investigation and response teams.</p>
<p>Mitigate risks to Personally Identifiable Information (PII) in its business processes and supporting systems through effective agency-wide implementation of corrective actions for processes</p>	<p>The SecureIT Guardium solution provides maximum visibility to database activity without impacting business processes. This provides additional measure of protection for mainframe and distributed platform database (SQL, Oracle, etc.) solutions by allowing management to customize violation reporting and alerts.</p> <p>The solution provides overall database security with a window into the security health with its Privacy Compliance Report Card and high level</p>

Federal Government Requirement	SecureIT Guardium Solution Summary
	graphical view of database users with a Sensitive Data Access Map.
Automate continuous monitoring of database security controls to support Certification and Accreditation (C&A)	The SecureIT Guardium Database Security Solution supports many of the NIST SP 800-53 security controls and automates continuous monitoring of these controls. <a href="#">Contact SecureIT for additional information.</a>

**Implement Database Security Best Practices**

Database Security Best Practice	SecureIT Solution Support
Step 1. Discover Assets	The SecureIT Guardium solution can discover all databases on the network. It can assess these databases for vulnerabilities and configuration compliance. It has a discovery feature to identify the sensitive data in the database and associated current security policy. The system can identify the applications that access the databases to construct a mapping of business applications to databases.
Step 2. Classify Policies	The SecureIT Guardium solution provides a database crawler to look for patterns such as 16-digit credit card numbers and 9-digit Social Security numbers in corporate databases. SecureIT can customize the database crawler to locate data specific to your agency. The system generates alerts when it locates sensitive data for the first time, helping organizations quickly identify business or IT processes that may result in the storage of sensitive OR PII data. The solution can be configured to automatically assign granular access policies to groups of objects, controlling who has access to them, from which applications and locations, at what times, using which SQL commands.
Step 3. Assess Vulnerabilities	<p>The SecureIT Guardium solution is only solution that enables enterprises to go beyond vulnerability reporting to address the entire vulnerability management lifecycle, including assessing business risk, supporting mitigation activities and streamlining compliance reporting and oversight processes.</p> <p>With the solution, you can pinpoint database vulnerabilities such as missing patches, misconfigured privileges, default accounts, and weak passwords create enormous risk. The solution incorporates an extensive library of assessment tests, based on industry best practices, to flag these and other static vulnerabilities. It also identifies dynamic or behavioral vulnerabilities—such as sharing of administration accounts and excessive administrator logins—by monitoring actual user activity over time. It includes embedded knowledge about enterprise applications such as Oracle EBS and SAP, to protect critical tables reserved for these applications (an essential control for SOX). A quarterly subscription service ensures that assessment tests are always up to date.</p>
Step 4. Continually Monitor for suspicious activity and policy violations	Unlike monitoring tools that only inspect inbound database commands, the SecureIT Guardium solution identifies unauthorized or suspicious actions by monitoring traffic both to and from database servers. Information collected by the Extrusion Policy Engine can also be used to understand the true extent

Database Security Best Practice	SecureIT Solution Support
	<p>of data theft, thus minimizing breach disclosure efforts and costs. Extrusion Policies can be used to detect activities by authorized users that fall outside normal business processes. The solution also provides access and security exception policies that monitor inbound database commands for unauthorized actions, such as SELECT operations by privileged users or failed logins that fall outside of a given threshold.</p>
<p>Step 5. Prioritize Threats</p>	<p>Prioritize remediation activities—based on business risk. Guardium automatically locates and classifies sensitive data such as credit card numbers in corporate databases, and analyzes baseline behavior to understand how and when line-of-business applications are accessing vulnerable databases. Risk assessment is crucial for prioritizing remediation, since most organizations do not have sufficient resources to patch all vulnerable systems at the same time.</p>
<p>Step 6. Fix Problems</p>	<p>The SecureIT Guardium solution protects unpatched systems with real-time controls. Vulnerable systems can take 3-6 months to patch. Our solution protects databases before and after they're patched, through database activity monitoring and signature-based policies, along with preventive controls such as real-time alerts, automated account lockouts and blocking. Policies and activity baselining can also protect against application vulnerabilities such as SQL injection and buffer overflow.</p> <p>Once vulnerable systems have been repaired using recommendations provided by the assessment tests, organizations need to ensure that only authorized changes are made. The SecureIT Guardium solution can be configured to prevent unauthorized changes to databases once a secure configuration baseline has been established.</p>
<p>Step 6. Log Capture, Analysis and Alert</p>	<p>The SecureIT Guardium solution creates a continuous, fine-grained audit trail of all database activities, including the “who, what, when, where, and how” of each transaction. This audit trail is contextually analyzed and filtered in real-time to produce the specific information required by auditors. The resulting reports demonstrate compliance by providing detailed visibility into database activities such as failed logins, escalation of privileges, schema changes, access during off-hours or from unauthorized applications, and access to sensitive tables. The solution provides proactive controls—such as real-time security alerts and blocking—to protect your critical data based on both predefined policies and anomaly detection.</p>
<p>Step 7. Measure Progress</p>	<p>Auditors want to know that incidents are being tracked and resolved in a timely manner. The SecureIT Guardium incident management and Compliance Workflow Automation modules allow you to track progress on the remediation of vulnerable systems and automate compliance report distribution, electronic sign-offs and escalations.</p> <p>The solution automatically generates compliance reports on a scheduled basis and distributes them to stakeholders for electronic approval. These reports—including escalations and sign-off reports—enable organizations to demonstrate the existence of an oversight process.</p>

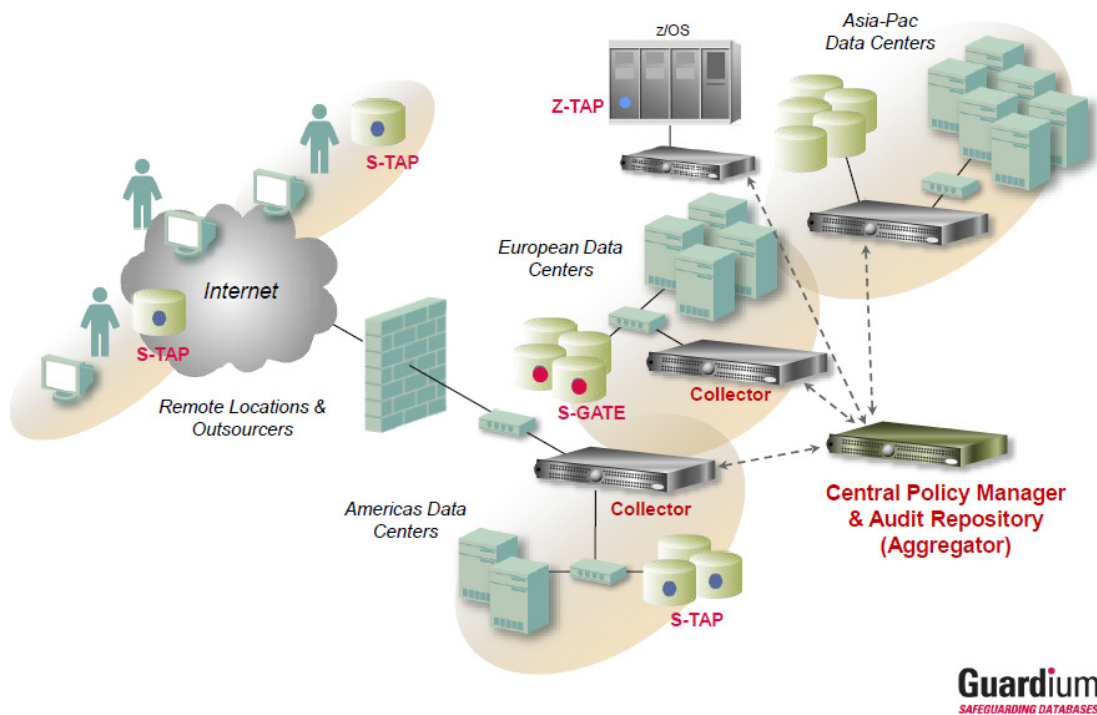
Database Security Best Practice	SecureIT Solution Support

***Enterprise Solution that can Scale***

Unique in the industry, Guardium’s multi-tier architecture automatically aggregates and normalizes audit information from multiple systems and locations into a single centralized repository. This enables enterprise-wide compliance reporting, correlation, forensics, and advanced database-focused analytics. A graphical Web console provides centralized management of policies, report definitions, compliance workflow processes, and appliance settings (such as archiving schedules). This scalable, multi-tier architecture can easily be scaled up to meet any mix of throughput and auditing policies, simply by adding appliances which work together in a federated model.

Guardium’s scalable architecture supports both large and small environments, with centralized aggregation and normalization of audit data, and centralized management of security policies via a Web console – enterprise-wide. S-TAPs are lightweight, host-based probes that monitor all database traffic, including local access by privileged users, and relay it to Guardium collector appliances for analysis and reporting. Collector appliances gather monitored data from S-TAPs and Z-TAPs (Z-TAPs are mainframe-resident probes) and/or by connecting directly to SPAN ports in network switches. Aggregators automatically aggregate audit data from multiple collector appliances. For maximum scalability and flexibility, you can configure multiple tiers of aggregators.

In order to support massive transaction volumes in enterprise data center environments, Guardium’s architecture incorporates patented, intelligent storage algorithms that provide 100x better storage efficiency than traditional flat file-based approaches. This allows you to significantly reduce storage costs while retaining more of your audit data online—in a centralized audit data warehouse that can be rapidly queried and mined for specific access patterns and transactions.



**Guardium**  
SAFEGUARDING DATABASES™

The Guardium architecture provides a range of non-intrusive deployment options to optimally match your environment. Database traffic is monitored using one of the following approaches:

- **S-TAP™ (Software Tap):** Unique in the industry, these lightweight, host-based software probes monitor both network and local database traffic (shared memory, named pipes, etc.) at the OS level of the database server. S-TAPs minimize any effect on server performance (typically 2-4%) by relaying all traffic to separate Guardium appliances for real-time analysis and reporting, rather than relying on the database itself to process and store log data. S-TAPs are often the preferred solution because they eliminate the need for dedicated hardware appliances in remote locations and outsourcing facilities (or access to available SPAN ports in your data center)
- **SPAN port or hardware tap:** In this configuration, the Guardium appliance is deployed as a non-inline, passive network monitor that captures a mirrored copy of the network stream by connecting to a SPAN port in your network switch, or a network tap.
- **Combination S-TAP and SPAN port:** For maximum flexibility, you can use a combination of host-based and network-based collection, depending on your network topology and relative ease of access to database servers and/or network switches

## Supported Platforms

Guardium's cross-platform solution is ideal for heterogeneous environments because it supports all major DBMS platforms and protocols running on all major operating systems. This table shows all currently supported platforms and versions.

Supported Platform	Supported Versions
Oracle	8i, 9i, 10g, 11g
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UDB (Windows) (Linux), (Unix), (z/Linux)	8, 9
IBM DB2 for z/OS	7, 8
IBM DB2 UDB for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10, 11
Sybase ASE	12, 15
Sybase IQ	12.6
MySQL	4.1, 5
Teradata	6.x, 12

Unique in the industry, S-TAPs are lightweight software probes that monitor both network and local database protocols (shared memory, named pipes, etc.) at the OS level of the database server. S-TAPs minimize any effect on server performance by relaying all traffic to separate Guardium appliances for real-time analysis and reporting, rather than relying on the database itself to process and store log data. S-TAPs are often preferred because they eliminate the need for dedicated hardware appliances in remote locations or available SPAN ports in your data center. This table shows all OS platforms and versions for which S-TAPs are currently available.

OS Type	Version	32-Bit & 64-Bit
AIX	5.1, 5.2, 5.3	Both
	6.1	64-Bit
HP-UX	11.00, 11.11	Both
	11.23, 11.31 PA	Both
	11.23, 11.31 IA	64-Bit
Red Hat Enterprise	2, 3, 4, 5	Both
Linux		
SUSE Linux	9, 10	Both
Enterprise		
Solaris - SPARC	6, 8, 9,10	Both
Solaris - Intel/AMD	10	Both
Tru64	5.1A, 5.1B	64-Bit
Windows	NT	32-Bit
	2000, 2003	Both

Guardium identifies potential fraud by tracking activities of end-users who access critical tables via multi-tier enterprise applications rather than direct access to the database. This is required because enterprise applications typically use an optimization mechanism called “connection pooling.” In a pooled environment, all user traffic is aggregated within a few database connections that are identified only by a generic application account name, thereby masking the identity of end-users. We support application monitoring for all major off-the-shelf enterprise applications. Support for other applications, including in-house applications, is provided by monitoring transactions at the application server level. This table shows all enterprise applications for which out-of-the-box support is provided, as well as all application server platforms that are supported.

**Supported Enterprise Applications**

Oracle E-Business Suite
PeopleSoft
Siebel
JD Edwards
SAP
Business Objects Web Intelligence
+ Others based on customer demand

**Supported Application Server Platforms**

(for other enterprise & custom developed applications)

IBM WebSphere
BEA WebLogic
Oracle Application Server (AS)
Microsoft .NET
JBoss Enterprise Application Platform
+ Others based on customer demand

## Case Studies

SecureIT has provided Cyber Security, Risk and IT Audit Services and IT solutions to Federal Government and other Major Organizations including:

- Federal Government: HHS, DOJ, Treasury, Commerce, Education, DISA, NASA, USAID, FTC, GAO, and USPS
- Financial Institutions: Freddie Mac, International Monetary Fund (IMF), Alliance Bank, E\*TRADE Financial, EXIM Bank, Inter-American Development Bank (IAB), and Riggs Bank
- Other Commercial Businesses: Beers & Cutler, CSC, DataPipe, HanleyWood, HMSHost, Noridian, Tier Technologies, Washington Post, and Watson Wyatt

The Guardium Solution is trusted by the world’s major institutions:

- Government: FRB, OCC, FDIC, FBI, and FTC
- Non-Government Organizations: Freddie Mac, WMATA
- Financial Services: 3 of top 4 global banks, top card brand
- Insurance: 3 of top 5 global insurance companies.
- Manufacturing: #1 beverage brand, #1 PC supplier, #1 automotive company.
- Telecommunications: 12 major telcos including 3 of top 10 worldwide.
- Retail & Hospitality: 2 of top 3 global retailers, major office brand, Wyndham Int’l.

- Software & Services: Leading BI vendor, ChoicePoint, Premiere Global Services.
- Energy: Global energy leaders including National Grid, Nevada Power, USEC.
- Health Care: Multiple BC/BS organizations.
- Media & Entertainment: Leading media including Discovery Communications.

### ***Washington Metropolitan Area Transit Authority (WMATA)***

As a tri-jurisdictional organization, WMATA operates the second largest rail transit system in the United States, and transports more than a third of the federal government to work and millions of tourists to landmarks in the Nation's Capital. According to a recent study of ridership trends, demand for WMATA service could grow anywhere from 50 to 100 percent by 2013. "Our customers trust us to transport them safely and safeguard their personal information," said Victor Iwugo, Chief of Metro IT Security (MITS), Department of Information Technology, WMATA. "Guardium has helped us implement robust, hardened 'security zones' around our critical production databases, with a DBMS-independent architecture that doesn't impact performance or require changes to our databases and applications."

WMATA selected Guardium to simplify what had been a complex and time-consuming initiative: achieving data security compliance in a complex, high-volume data center environment. With Guardium, WMATA is now able to secure personal sensitive data and can pass audits more quickly and easily. At the same time, the Guardium solution enables WMATA to simplify enterprise security by automating and centralizing the most challenging controls required for compliance, including:

- Protecting stored data with granular access controls based on parameters such as source application, IP address, and other criteria
- Maintaining systems in accordance with established security configuration best practices
- Restricting access to sensitive information
- Tracking and monitoring all access to personally identifiable information (PII)

### ***Financial Services Firm with 1M+ Sessions/Day***

A global NYSE-traded company with 75M customers needed to improve database security for SOX compliance & data governance. Using a two phase approach, the Guardium database security solution was implemented to monitor all privileged user activities, especially DB changes and address requirements for data privacy.

The environment consisted of four (4) data centers managed by IBM Global Services

- 122 database instances on 100+ servers
- Oracle, IBM DB2, Sybase, SQL Server on AIX, HP-UX, Solaris, Windows
- PeopleSoft plus 75 in-house applications

Alternatives such as native database auditing was considered but determined not practical because of performance overhead as DB servers were already at 99% capacity.

**Results:**

- Auditing 1M+ sessions per day (GRANTS, DDLs, etc.)
- Caught DBAs accessing databases with Excel & shared credentials
- Producing daily automated reports for compliance; sign-off by DBA & CISO teams
- Automated change control reconciliation using ticket IDs
- Passed 2 external audits

## About SecureIT

[SecureIT](#) is a professional and technical services firm focusing on information security and risk management. SecureIT helps Federal government agencies, corporations and other non-government organizations manage risks in business processes, technology and contracted services through services and solutions in the areas of [Cybersecurity](#), [Information Assurance](#), [Governance, Risk & Compliance](#), [IT Audit](#), and Security Training. Founded in 2001, the company sits on the board and is active in Washington DC area chapters of information security organizations such as ISACA, ISSA and IIA. SecureIT serves clients in the Federal government including: DISA, HHS, DOJ, Treasury, USAID, Education, NASA and USPS as well as corporations such as Beers & Cutler, Constellation Energy, CSC, E\*TRADE, Noridian, and The Washington Post in addition to non-government organizations such as Freddie Mac Inter-American Development Bank and the International Monetary Fund (IMF).

For more information, call 703.464.7010, email [info@secureit.com](mailto:info@secureit.com) or visit [www.secureit.com](http://www.secureit.com)

## Notice

The SecureIT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice. Information used in the production of this paper also courtesy of Guardium.