

# Guardium Appliance - Collector

## Real-time database security and data governance

### Highlights

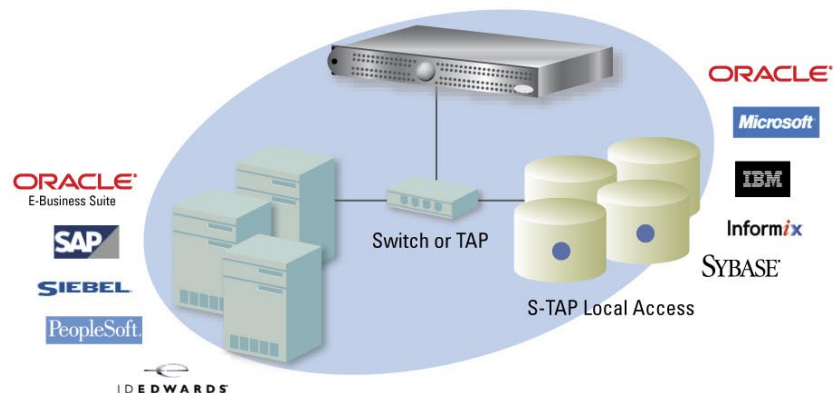
- Out-of-the-box solution that both protects databases in real time and automates the entire compliance auditing process
- Non-invasive, appliance-based technology can be up and running in minutes – with virtually zero impact on performance, stability, or operations
- Hardened appliance built on a high-performance, high-availability, industry-standard server platform
- Unified, cross-platform solution that's designed for heterogeneous environments
- Optional lightweight software agent (S-TAP) installed on database servers to monitor both network and local database traffic at the OS level
- Easily scalable architecture designed to meet any mix of workload and distributed monitoring criteria

Unlike traditional database logging solutions, Guardium delivers a network-resident solution that uniquely combines real-time database security with fully automated compliance auditing process. This solution is an appliance-based approach that allows organizations to rapidly meet auditors' requirements, reduce compliance costs, and protect critical data – without impacting applications, databases, or networks.

Guardium's G1000 and G2000 appliances are hardened 1U rack-mountable units built on a high-performance, industry-standard server platform. These self-contained systems enable you to efficiently monitor, collect, report, and manage all database access activities.

The appliance non-invasively inspects the data stream and enables monitoring of all database access activities, with continuous fine-grained auditing and reporting, real-time policy-based alerting, and passive blocking (via TCP reset) of unauthorized database access. It supports a range of network deployment options: network hub, SPAN port, network TAP, and S-TAP (a lightweight software agent installed on database servers).

The system also monitors privileged local traffic – such as SSL console access, shared memory, and named pipes – at the operating system IPC layer via an S-TAP.



In order to enforce separation of duties, all audit data is stored in a secure, tamper-proof repository internal to the Guardium appliance. There is no root access to the appliance and all audit data is encrypted when it's archived to external storage devices.

The Guardium architecture can easily be scaled up to meet any mix of workload and distributed monitoring criteria. In enterprise data center environments, you can deploy multiple appliances in a multi-tier topology. In this case, a central management appliance, G5000, aggregates and analyzes audit data, distributes reports, and manages enterprise-wide security policies as one federated system.

## Guardium G1000 & G2000 Appliance Specifications

<b>Product Description</b>	Hardened appliance for real-time database security and continuous auditing		
<b>Operational Modes</b>	Privileged Access Monitoring Selective Auditing and Alerting Comprehensive Auditing		
<b>Alerts</b>	Mail, SNMP, SYSLOG, and custom Java class notification; real-time and statistical threshold alerts		
<b>Administration &amp; Setup Interface</b>	HTTPS, SSH and Console		
<b>High Availability Features</b>	Multi-LAN; hot-plug RAID-1 protected internal storage; hot-plug redundant power supply (G2000)		
<b>Database Platforms</b>	<b>Platform</b>	<b>Version</b>	
	Oracle	8i, 9i, 10g r1, 10g r2	
	Sybase ASE	12, 15	
	Sybase IQ	12.6	
	MS SQL Server	2000, 2005	
	Informix	7, 9, 10	
	DB2 UDB	8, 9	
<b>File Servers</b>	FTP, Windows File Share		
<b>OS Platforms (S-TAP)</b>	<b>OS</b>	<b>Version</b>	
	Solaris	8,9,10	
	AIX	5.1, 5.2, 5.3	
	HP-UX	11.00, 11.11, 11.23 PA, 11.23	
	Tru64	5.1A, 5.1B	
	Linux	2.4.x & 2.6.x kernels	
	Windows	NT, 2000, 2003 IA32, IA64, x64	
<b>Enterprise Applications</b>	Oracle EBS, PeopleSoft, Siebel, SAP		
<b>Software Modules (optional)</b>	Archiving Extension Enabler; External Data Connector; AuditGuard; HealthGuard; PolicyGuard Access Monitoring; PolicyGuard Extrusion Controls; Integrated Incident Manager; Change Audit System; Database Content Classifier		
<b>Compliance Accelerators (optional)</b>	SOX, PCI, Data Privacy		
<b>Hardware</b>	<b>G1000</b>	<b>G2000</b>	
	Form Factor	1U	1U
	CPU & Cache	One Dual Core Xeon Processor 3050, 2MB Cache, 2.13GHz, 1066MHz FSB	Two Dual Core Xeon Processor 5140, 4MB Cache, 2.33GHz, 1333MHz FSB
	Memory	2GB 667MHz	4GB 667 MHz
	Network Interface Types	Copper/Fiber; Up-to 6 ports	Copper/Fiber; Up-to 10 ports
	Network Speeds	10/100/1000 Mbps	10/100/1000 Mbps
	Internal Storage	Two 146GB, SAS, 3.5-inch 10K RPM, RAID-1	Two 146GB, SAS, 3.5-inch 10K RPM, RAID-1
	Power	Single 345 Watts, 110/220 volts non-redundant	Dual 670 Watt, 110/220 volts, redundant, hot-plug, auto-switching

**Guardium®**  
SAFEGUARDING DATABASES™

230 Third Avenue • Waltham, MA 02451 USA • T: +1 781 487 9400 • F: +1 781 487 7900 • www.guardium.com

✓ *Secure enterprise data* ✓ *Pass the audit*

Copyright © 2007 Guardium. All rights reserved. Information in this document is subject to change without notice. Guardium, Safeguarding Databases, S-TAP are trademarks of Guardium. All other trademarks and service marks are the property of their respective owners.