

## Automated Database Activity Monitoring, Auditing and Vulnerability Assessment

### Knowledge is Power

Databases store some of the most highly sensitive customer and business data in the enterprise. However, while network security has become established practice, database security has often been overlooked. To meet the growing demand for more pervasive access to database applications that expose the database to more people and applications, database administrators (DBAs) are increasingly faced with security issues that rival network security—including insider threats, and rising data breach costs for compromised or lost records. As a result, securing the database has become integral to protecting any enterprise infrastructure, with regulators stepping in to review database-specific security compliance. Enforcing acceptable use policies, identifying and blocking new database security threats, and complying with emerging industry and governmental regulations regarding privacy and disclosure of security practices requires sophisticated database activity monitoring (DAM) and vulnerability assessment (VA) capabilities.

### Solutions for Dynamic Security Management

The FortiDB Family of products provide centrally managed, enterprise-scale, database hardening features with fast, comprehensive policy compliance with database activity monitoring and vulnerability assessment for improved data security across the enterprise. DBAs realize quick time-to-value with easy to install, intuitive, high value standard compliance policies (PCI-DSS, SOX, GLBA, HIPAA) and reports ready out-of-the-box to ensure database regulatory compliance requirements are met. FortiDB dedicated hardware appliances easily plug into the network for fast deployment. FortiDB provides full-featured monitoring and auditing technology used by companies around the world to address critical issues such as Change Control, Internal Controls, Privileged User Monitoring, and Privacy Protection. Automation through scheduling and scripting dynamically detects database security weaknesses and non-compliance with standard policies. Appliances are pre-populated with hundreds of policies that cover standard industry and governmental requirements, and security best practices. A comprehensive set of standards-based graphical reports are built into the system to produce immediate results.

### Key Solution Features and Benefits

<ul style="list-style-type: none"> <li>Full Database Activity Coverage</li> </ul>	Captures all types of database activity from administration events to user activity, regardless of originating command type (plain SQL or stored procedures) or connection type (ex - standard, pooled, or console).
<ul style="list-style-type: none"> <li>Automatic Database Discovery</li> </ul>	High-performance scans quickly find all databases on the network and across WAN and subnet boundaries—even on irregular ports.
<ul style="list-style-type: none"> <li>Accelerated Security and Compliance Best Practices (PCI, SOX, HIPAA)</li> </ul>	Automatic updates to latest regulatory / industry best practices add to hundreds of pre-populated security and compliance policies.
<ul style="list-style-type: none"> <li>Centralized Policy Management</li> </ul>	Centralized web-based access allows DBAs to more quickly identify and react to database security threats across the network.
<ul style="list-style-type: none"> <li>Business-Driven Assessments with Flexible Sets of Policies</li> </ul>	Easily run policies to verify that databases conform to corporate standard configurations, implement tests for custom applications, or conduct Extended Penetration Testing to test for common passwords, etc.
<ul style="list-style-type: none"> <li>Standardized Compliance Reports with Trend Analysis</li> </ul>	Standardized, exportable audit reports customizable with company branding are designed out-of-the-box to support compliance programs, with graphic trend analysis to spot and isolate patterns.
<ul style="list-style-type: none"> <li>Enterprise Scalability</li> </ul>	Supports flexible deployments across the network of multiple databases per appliance for consistent enterprise-wide policy enforcement, processing tens of millions of audit records from databases per day.



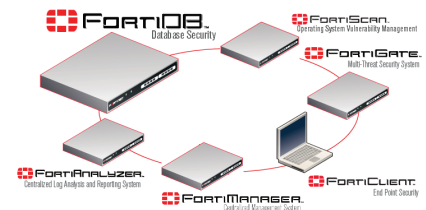
FortiDB appliances



Fortinet Database Security Software

### Low Impact Total Cost of Ownership (TCO)

Failing to keep up with today's regulations for data security can be cost prohibitive. FortiDB simplifies the process with regular policy and signature updates via XML, and current industry leading remediation advice that strengthens the integrity and security of databases—mitigating internal threats, managing database vulnerabilities to prevent costly breaches, and improving visibility of access policy security violations. Native audit guarantees a 100% capture rate. And the low impact, non-intrusive agent-less architecture simplifying deployment does not interfere with database operations or put applications at risk.



## Database Activity Monitoring & Auditing with FortiDB— Complete, Accurate Audit Trails

### Full Database Activity Capture for Auditors

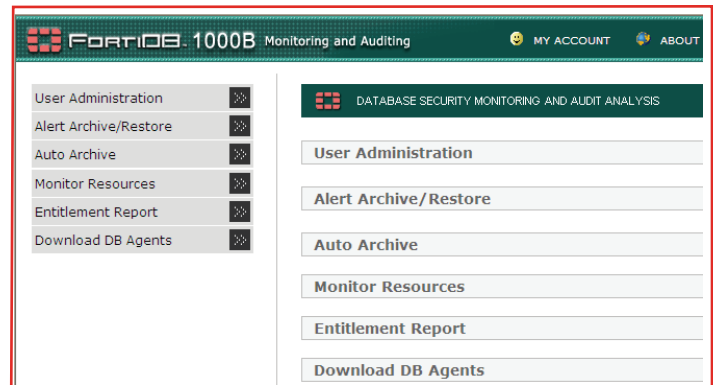
Incomplete and inaccurate information compromises both compliance and security. FortiDB captures all database activity in a security and compliance context for specific behaviors that might, for instance, indicate a SQL injection attack or inappropriate access by a privileged user.

Network security at the perimeter is not enough. Some experts say privileged users account for 78% of the threat. While there are tools that look at network traffic to try to deduce database activity, network monitoring of the database has some shortcomings in terms of capturing stored procedures, some connection types, encryption, aborted long-running transactions, and server-only activity among other things. For instance, network sniffers cannot tell whether the stored procedure “sp\_ignoreme” is deleting every transaction in an order entry table or modifying user privileges.

In contrast full monitoring with FortiDB captures all types of database activity. In order to meet the compliance requirements, businesses must implement controls that prevent erroneous data or prevent misuse of data. For these controls to be effective, they must be operational 24x7.

Continuous database monitoring:

- Continuous database monitoring or schedule-based monitoring
- Captures all types of database activity from administration events to user activity
- Captures all changes whether the originating commands were plain SQL or stored procedures
- Captures activity irrespective of connection type (ex - standard, pooled, or console)
- Captures activity on encrypted networks without requiring bypasses
- Captures full activity, including metadata changes, privilege changes, data changes, content changes and user behavior



### Behavioral and Content Analysis

FortiDB can also learn user behavior, not only in support of IPS network-based tools like those in FortiGate, but also to detect and prevent anomalous database queries by authorized users. FortiDB learns user behavior and discovers when activities fall outside of normal behavior, including suspicious access frequency, suspicious logins, excessive reads and abnormally long sessions. By correlating database activities across multiple databases and learning what is appropriate content using probabilistic modeling, FortiDB discovers unusual or unexpected data values, and verifies that input from applications and batch jobs matches expectations.

### Accurate Audit Trails

Selected by some of the world's leading security compliance auditors, Database Auditing with FortiDB records database activity for complete and accurate audit trails—including internal audits of FortiDB itself. Independent audit storage provides an additional security layer for audit integrity. Alerts can be individually provided to email, paging, and control centers.

### FortiDB Compliance Policy Assessment and Reporting Features

FortiDB supports the following compliance policy assessment and reporting features:

- **Standardized Regulatory and Industry Policies** FortiDB is pre-populated with hundreds of policies for accelerated security and compliance to address multifaceted security standards, including PCI-DSS, SOX, GLBA, HIPAA. Best practices, known database exploits, database related operating system issues, and database access privileges are also covered.
- **Central Repository** The central repository stores all vulnerability data—or thousands of databases and even more scans—and enables trend analysis, easy report distribution, and consistent policy enforcement across the IT landscape.
- **Separation of Duties** Based upon your business needs, FortiDB can create users with different roles, separating system administrator roles from assessment, policy or report manager roles, for instance.
- **Web-based Interface** A web-based interface that users can access via web-browsers allows for easy access from remote locations and reduced IT costs for end-user installation.
- **Command Line Interface** For added flexibility, along with the intuitive web-based user interface administrators can automate vulnerability assessment and administration tasks using the FortiDB Command Line Interface (CLI).
- **SNMP support** Simple Network Management Protocol (SNMP) support facilitates the exchange of management information between network devices to provide integration with Ticket, Change, and Configuration Management systems for closed-loop processes.

### AN AUTOMATED PROCESS

Without an automated database security solution, important database changes and policy breaches could easily go unnoticed, affecting the reliability of financial data and more, e.g., automated checks on running supported versions, specified patch levels, and complying with secure configuration settings. Automation allows for more frequent assessments, broader database coverage, improved availability, and added confidence in repeatable and demonstrable policy compliance without increasing labor costs.

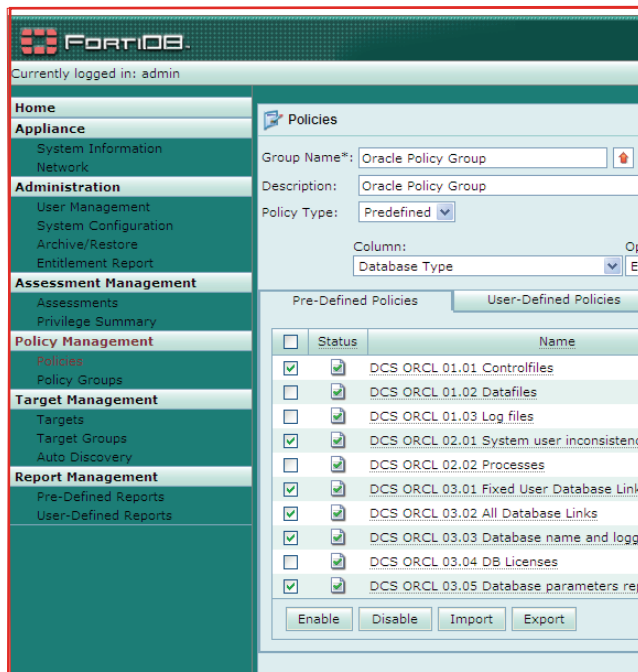
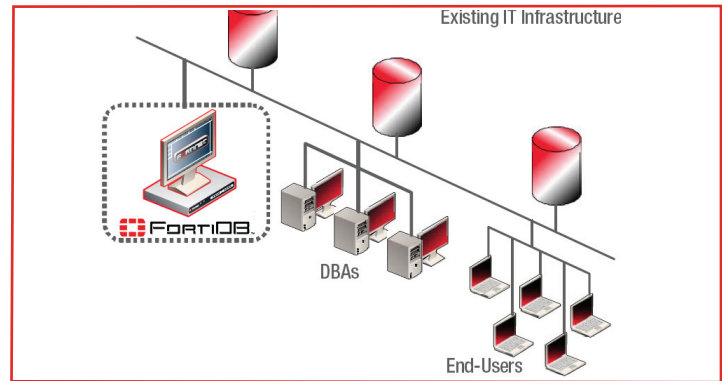
### INSIDER THREAT ASSESSMENT

Privileged User Assessment and Separation of Duties mitigate insider threats, assessing permissions, user passwords, structures.

## Centralized Vulnerability Assessment with FortiDB— Compliance Policy Enforcement and Reporting

### Understanding the Dynamic Security Environment

While many companies implement network security as the main guard against security compromises, often the target of these attacks is the most often overlooked network asset—the database. Databases need to be scanned regularly for vulnerabilities just like other IT assets. Understanding how databases fit into an effective security policy is key to protecting some of the most business-sensitive data in the enterprise. FortiDB eases this process, automating a manual process for consistent application of database security policy, verifying that databases conform to corporate standard configurations, and even conducting Extend Penetration Testing to test for passwords commonly used within an organization.



### Keeping up with Compliance—PCI-DSS, SOX, GLBA, HIPAA

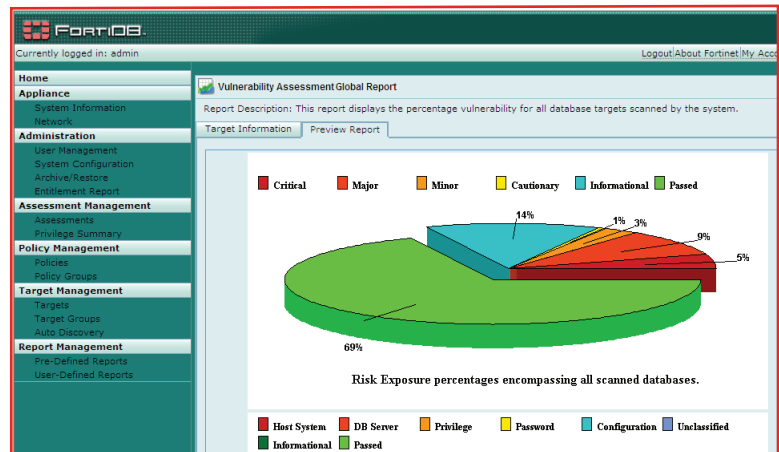
New regulatory, compliance and legal mandates largely in response to headline-grabbing security breaches and accounting scandals require businesses to not only understand database events, but also proactively implement and enforce database security policy. Selecting a compliance solution that keeps up with the latest industry and regulatory compliance requirements with periodic fully automated updates like FortiDB simplifies the process.

Separation of Duties—important for all compliance standards—allows unique access privileges and rights to be assigned to different FortiDB users based on requirements and needs. FortiDB takes care of 9 of the top 12 Payment Card Industry Data Security Standard (PCI-DSS) requirements, more with FortiGate UTM Firewall protection. FortiDB also supports database compliance with risk assessment to help establish an environment of accountability as required by sections 302, 404, and 409 of the Sarbanes-Oxley (SOX) act. Similarly, FortiDB pre-defined policies for commercial and investment banks simplify compliance with provisions of the Gramm-Leach-Bliley Act (GLBA).

Comprehensive security and privacy policies in FortiDB address the large regulatory burden that the Health Insurance Portability and Accountability Act (HIPAA) places on organizations that deal with certain types of health-related information, including security of electronic protected health information (ePHI).

### Security Reporting—Security Management

FortiDB addresses the analysis and reporting challenges in today's complex regulatory environments. Implemented on a scalable, high-performance platform, FortiDB allows DBAs to capture security compliance information from their entire network of distributed, heterogeneous databases. Pre-defined detailed, summary, global, and trend reports can be exported to PDF, Excel, Comma Separated Values (CSV) and Tab-Delimited formats for use with third party tools. Administrators can group by a specific policy or target, e.g., policy severity or target port, and a whole host of customization options for company branded User-Defined Reports. Templates reserve space for business names and logos. FortiDB supports more effective security management with intelligent reports to assess database security posture at a glance.



## TYPICAL APPLICATIONS

FortiDB-400B

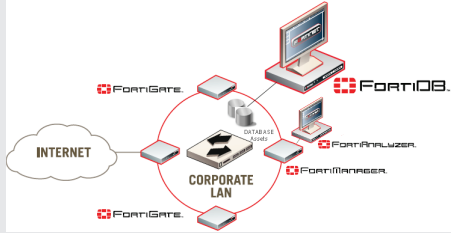
FortiDB-1000B

FortiDB-1000B

FortiDB-2000B

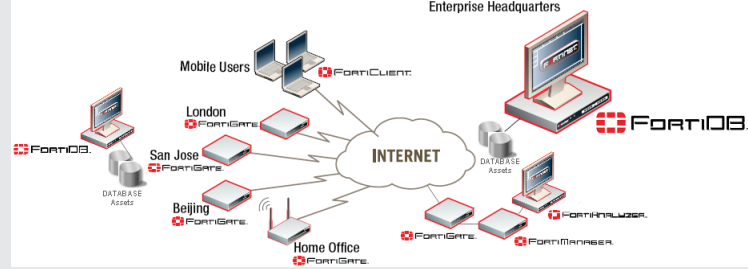
Fortinet Database Security Software

1-10 or 1-30 Database Instances  
Distributed, Heterogeneous Database Network



Small-Medium Enterprise Network  
with Central Corporate LAN

1-30 or 1-60 Database Instances  
Remote Offices and Branches



Medium-Large Enterprise Network with Distributed Databases

### FortiDB Models



Feature	FortiDB-400B	FortiDB-1000B	FortiDB-2000B
Security Hardened Platform.....	Yes	Yes	Yes
Number of Licensed Database Instances.....	10	30	60
10/100/1000 Ethernet.....	4	4	4
RAM .....	2 GB	2 GB	4 GB
Number of Hard Drives .....	1	1	1
Total Hard Drive Capacity.....	500 GB (1 TB option)	1 TB (2 TB option)	1 TB (6 TB option)
Storage key (boot image).....	1 GB Compact Flash	1 GB USB	1 GB USB
RAID Storage Management.....	No	No	No
Redundant Hot Swap Power Supplies.....	No	No	Yes
Dimensions (H, W, L) .....	1.7 x 17.25 x 14.5 in. (4.5 x 43.8 x 36.8 cm)	1.7 x 16.7 x 30.4 in. (4.3 x 42.6 x 77.2 cm)	3.5 x 17.5 x 27.5 in. (8.9 x 44.5 x 69.8 cm)
Weight.....	10 lbs (4.5 kg)	35.8 lbs (16.3 kg)	55.3 lbs (25.1 kg)
Rack Mountable.....	Yes	Yes	Yes
AC Power Required.....	100-240 VAC, 50-60 Hz, 4.0 Amp (Max)	100-240 VAC, 50-60 Hz, 4.8Amp (Max)	100-240 VAC, 50-60 Hz, 9.4 Amp (Max)
Auto-switching universal.....	110/220 Volts	110/220 Volts	110/220 Volts
Average Power Consumption.....	121 Watts	275.4 Watts	316.9 Watts
Operating Temperature .....	32 to 104 deg F (0 to 40 deg C)	50 to 95 deg F (10 to 35 deg C)	50 to 95 deg F (10 to 35 deg C)
Storage Temperature .....	-31 to 158 deg F (-35 to 70 deg C)	-40 to 149 deg F (-40 to 65 deg C)	-40 to 149 deg F (-40 to 65 deg C)
Humidity .....	20-90% non-condensing	5-95% non-condensing (twmax=38C)	20-80% non-condensing
Regulatory .....	FCC Class A, CE, UL/CB/CUL	FCC Class A Part 15 / CE Mark	FCC Class A Part 15 / CE Mark

### Fortinet Database Security Software

Security Hardened Platform.....	Yes
Number of Licensed Database Instances.....	Licensed per database
System Requirements .....	2.0 GHz CPU, 1024 MB RAM, 200 MB HDD
Operating System support.....	AIX 5.3 (64-bit); Red Hat Enterprise Linux 4.0 or 5.0 (64-bit); Solaris 10 (64-bit); Windows XP / Vista; Windows Server 2003, SP1 (32-bit or 64-bit)

### All Fortinet Database Security Products

Database support.....	DB2 UDB V8 (except UBM object policy), DB2 UDB V9 (VA only); MS SQL Server 2000 MS SQL Server 2005, MS SQL Server 2008; MySQL 5.1 (VA only); Oracle 9.2.x, .... Oracle 10gR1, Oracle 10gR2, Oracle 11.1.0.x; Sybase ASE 12.0 (DAM only), .... Sybase ASE 12.5, Sybase ASE 15.0.2 (VA only)
Repository Database support.....	Apache Derby 10.x, DB2 UDB v9, Microsoft SQL Server 2005, Oracle 10gR2, .... PostgreSQL 8.3
Browser support .....	Internet Explorer 7.x, Firefox 2.x (VA only), Firefox 3.x (VA only)

### FortiCare™ Support Services

- 24 x 7 x 365 FortiCare Web Service <sup>[1]</sup>
- 8x5 Web-Based Technical Support <sup>[2]</sup>
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

<sup>[1]</sup> Annual renewal required to maintain service

<sup>[2]</sup> 24 x 7 Telephone Technical Support available.

### About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection—including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam—designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: firewall, antivirus, IPSec, SSL, network IPS and anti-Spyware. Fortinet is privately held and based in Sunnyvale, California.

## FORTINET

### GLOBAL HEADQUARTERS

Fortinet Incorporated  
1090 Kifer Road, Sunnyvale, CA 94086 USA  
Tel +1-408-235-7700  
Fax +1-408-235-7737  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

### EMEA SALES OFFICE-FRANCE

Fortinet Incorporated  
120 Rue Albert Caquot  
06560 Sophia Antipolis, France  
Tel +33-4-8987-0510  
Fax +33-4-8987-0501

### APAC SALES OFFICE-SINGAPORE

Fortinet Incorporated  
61 Robinson Road, #09-04 Robinson Centre  
Singapore 068893  
Tel: +65-6513-3730  
Fax: +65-6223-6784

Copyright© 2009 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600. FDB-R1D5-0409-4P