

FortiDB™

Database Security and Compliance

Automated Security and Compliance

The FortiDB family of appliances and software delivers a complete Database and Application security product line. It delivers centrally managed security, audit policy compliance and Vulnerability Management (VM) for databases and applications across your extended enterprise. FortiDB enables you to meet the challenges of increasing access to your business-critical data in ERP, CRM, or SCM systems while decreasing the threat of data breach. Its sophisticated database activity monitoring (DAM) and advanced reporting automatically documents your policy compliance with internal policies as well as government or industry regulations such as PCI-DSS, SOX, Basel II, GLBA, and HIPAA.

Comprehensive Monitoring and Audit

FortiDB enforces acceptable use policies and alerts on database security threats. It continuously monitors all access to personally identifiable data (PID) residing in your databases. FortiDB's full-featured monitoring and auditing technology manages critical tasks such as change control, internal controls, privileged user monitoring, privacy protection and policy based auditing. Its change control features keep track of all changes related to database structures and users. This includes both Data Definition Language (DDL) and Data Control Language (DCL). FortiDB also automatically generates user activity baselines for easy policy configuration. FortiDB provides three collection methods - Selective Native Audit, Network Sniffer and Agents. Allowing to utilize all three methods within the same installation, FortiDB provides greater flexibility than any other product

Detect Weaknesses Automatically

FortiDB's Vulnerability Management features automatically detects new security weaknesses, policy noncompliance. In addition, customers can scan their networks to detect and discover new databases and a Sensitive Data Discovery function allows identifying database elements that hold sensitive data such as credit card numbers, Social Security numbers and much more. FortiDB appliances and software ship with hundreds of pre configured policies that address industry and governmental compliance requirements, as well as security best practices. They include a comprehensive set of standards-based reports that provide specific, actionable information. The FortiGuard Global Threat Research Team provides dynamic policy and signature updates. This industry-leading research and remediation advice enables you to strengthen the integrity and security of your databases quickly and effectively.



FortiDB Eases Regulatory Compliance

- ✓ Sensitive data discovery; aids in PCI-DSS compliance
- ✓ Periodic scan of every Database in your network
- ✓ Automatic user activity baseline generation for easy configuration
- ✓ Built-in best practices for regulations such as SOX
- ✓ Out of the box policies for both Security and Audit
- ✓ Flexible deployment and web-based management
- ✓ Flexible audit data collection methods - native auditing, network sniffer or light-weight agents
- ✓ Independent and secure audit storage
- ✓ Comprehensive Audit/Compliance reports
- ✓ Automated policy updates by FortiGuard services

Features	Benefits
Centralized policy configuration and enforcement	Simplifies the creation and enforcement of data protection policies, which reduces the risk of data loss while increasing policy compliance.
Assessment	Provides remediation advice after vulnerability scans. Discovers sensitive data in databases. Also establishes user activity Baselines for more efficient policy configuration.
Captures all types of database activities (Selects, DMLs, DDLs and DCLs)	Captures database activities, either utilizing the native audit, network protocol agents, or network sniffers. Alerts can be sent via SNMP, SMTP and SYSLOG to SEIM products.
Automation of compliance	Captures audit data from heterogeneous environments for automated compliance reporting.
Supports virtualized environments	Ensures comprehensive policy compliance enforcement in both virtualized and standard environments.

The FortiDB Family



FortiDB-400B



FortiDB-1000C



FortiDB-2000B

System Administration Target Database Server Policy Vulnerability Assessment **DB Activity Monitoring** Report

Target DB Activity Profiling: oracle_11g2_10.101.0.60

DB Login/User: SYSTEM (7) Source Applications: 1 Tables Accessed: 7

Source IP	OS Hostname	Source Application	OS User	Session Count
10.101.0.1	foundert-328f1	SQL Developer	xiangfan	1

Displaying item 1 of 1.

Table Name	Select	Update	Insert	Delete	Create	Alter	Drop	Trunc	Grant	Revoke
oracle.SYSTEM.student	0	0	0	0	1	0	1	0	0	0
oracle.SYSTEM.v_st	0	0	0	0	1	1	1	0	0	0
oracle.scott.emp	0	0	0	0	0	0	0	0	1	1
oracle.SYSTEM.employee	0	0	0	0	1	0	1	0	0	0
oracle.SYSTEM.tab_test_ddl_2	0	0	0	0	1	0	1	0	0	0
oracle.SYSTEM.department	0	0	0	0	1	0	1	0	0	0
oracle.SYSTEM.tab_test_ddl	0	0	0	0	1	4	1	0	2	2

Displaying items 1 thru 7 of 7.

Refresh Back

Activity Profiling

FortiDB automatically generates user activity baselines for easy policy configuration.

System Dashboard Policy Vulnerability Assessment DB Activity Monitoring Report

Target Database Server

Target Database Server Defined: 9
 Database Server Define Complete: 9
 Database Server Define Incomplete: 0
 Database Server Group: 5
 License Limit of Database Server: 30

Policy

Total Policies (VA/DAM): 655/45
 VA Pre-Defined Policies: 651
 VA User-Defined Policies: 4
 Policy Groups(VA/DAM): 11/11
 Last VA Pre-Defined Policy Update: 06/30/11

Vulnerability Assessment

Assessment Defined: 7
 Currently Running: 0
 Scheduled: 0
 Assessment Run: 13
 Total Vulnerability Result: 196
 Vulnerabilities Found: 47
 Informational Result: 45
 Check Passed: 104

VA Vulnerabilities

By Severity: Critical: 16 (8.5%), Major: 19 (17.0%), Minor: 8 (4.0%), Cautionary: 4 (2.1%)

By Classification: Host System: 2 (0.0%), DB Server: 14 (29.8%), Privilege: 7 (14.9%), Password: 10 (21.3%), Configuration: 10 (20.8%), Unclassified: 0 (0.0%)

DB Activity Monitoring

Target Allow Monitor: 9
 Currently Monitoring: 2
 Alerts Grouping: 10
 Grouping Scheduled: 0
 Total Alerts: 638744
 Today: 36899
 Recent 7 Days: 638744
 Recent 30 Days: 638744
 Recent 12 Months: 638744

Recent DAM Alerts

Week Month Year

Dashboard

FortiDB's dashboard displays essential Vulnerability Assessment and Database Activity Monitoring/Audit information.

System Administration Target Database Server Policy Vulnerability Assessment **DB Activity Monitoring** Report

Alerts Summary

DB Activity Monitoring

Total Alerts: 640717
 Today: 36872
 Recent 7 Days: 640717
 Recent 30 Days: 640717
 Recent 90 Days: 640717
 Recent 12 Months: 640717

Target Allow Monitor: 9
 Currently Monitoring: 2
 Alerts Grouping: 10
 Grouping Scheduled: 0

Recent 7 Days:

Recent 30 Days:

Recent 90 Days:

Recent 12 Months:

By Severity:

Severity	Count
Informational	26205

By Policy:

Policy Name	Count
My Alert user Policy	12350
Export-userPolicy	10403
My Alert table Policy	810
My Alert table column Policy	810
My Alert session Policy	552
Tables	405
Table Privileges	270
Tablespaces	270
xfan.sessionPolicy	254
System Privileges	32
sessionPolicy1	32
4.2.1-userPolicy	10
Export-tablePolicy	4
4.2.1-sessionPolicy	2
Export-tableColumnPolicy	1

By Action:

DB Action	Count
SELECT	21683
INSERT	1082
LOGON	596

Alert Summary

High level overview of alerts and trends.

Alerts Analysis

Detailed trend analysis allows users to improve their internal control infrastructure.

FortiDB	FortiDB-400B	FortiDB-1000C	FortiDB-2000B
Hardware Specification			
Security Hardened Platform	Yes	Yes	Yes
Number of Licensed Database Instances	10	30	60
10/100/1000 Interfaces	4	4	4
RAM	2 GB	3 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
Redundant Hot Swappable Power Supplies	No	No	Yes
Hardware Form Factor	Rack Mount (1-RU)	Rack Mount (1-RU)	Rack Mount (2-RU)
Dimensions			
Height	1.7 in (4.5 cm)	1.69 in (4.3 cm)	3.5 in (8.9 cm)
Width	17.25 in (33.7 cm)	17.09 in (43.4 cm)	17.5 in (43.8 cm)
Length	14.5 in (36.8 cm)	24.7 (62.71 cm)	27.5 in (69.8 cm)
Weight	10 lbs (4.5kg)	24.2 lbs (11 kg)	55.3 lbs (25.1 kg)
Environment			
AC Power Required	100 – 240 VAC, 50 – 60 Hz, 4.0 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 7 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 9.4 Amp (Max)
Power Consumption (AVG)	121 W	189 W	317 W
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)	50 – 94 deg F (10 – 35 deg C)
Storage Temperature	-31 to 158 deg F (-35 – 70 deg C)	-40 to 149 deg F (-40 – 65 deg C)	-40 to 149 deg F (-40 – 65 deg C)
Humidity	20 to 95% non-condensing	5 to 95% non-condensing	20 to 80% non-condensing
Compliance			
	FCC Class A, CE, UL/CB/CUL	FCC Class A Part 115 / CE Mark	FCC Class A Part 115 / CE Mark
Supported Platforms			
Database	DB2 UDB V8 (VA only), DB2 UDB V9.x (VA only), DB2 UDB V9.5, DB2 UDB V9.7, MS SQL Server 2000, MS SQL Server 2005, MS SQL Server 2008, MySQL 5.1, Oracle 9i, Oracle 10 gR1 (VA only), Oracle 10gR2, Oracle 11g, SybaseASE 12.5 (VA only), Sybase ASE 15.x		
Repository Database	Apache Derby 10.x, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Oracle 10gR2, Oracle 11g, PostgreSQL 8.3		
Browser	Internet Explorer 7,8; Firefox 3,4,5		

FortiDB Software

Fortinet also gives you the ability to deploy FortiDB database security software on a range of software platforms. You can install FortiDB on Red Hat Linux, AIX, Solaris 10, Windows XP/Vista, Windows Server 2003, as well as virtualized environments. FortiDB software delivers the same centralized policy management for vulnerability management and database activity monitoring as FortiDB appliances.

Complete Security Solution

FortiDB is part of Fortinet's comprehensive portfolio of security gateways and complementary products that deliver a powerful blend of integrated multi-threat protection, ASIC-accelerated performance, and constantly updated, in-depth threat intelligence.

This unique combination delivers the highest level of network, content, and application security for organizations of all sizes, including managed service providers and telecommunications carriers. Fortinet's integrated approach improves your security posture while reducing your total cost of ownership and providing you with a flexible, scalable path for expansion.

The Fortinet portfolio includes:

- FortiGate® Network Security
- FortiAnalyzer™ Centralized Reporting
- FortiMail™ Messaging Security
- FortiManager™ Centralized Management
- FortiClient™ Endpoint Security
- FortiWeb™ Web Application Security
- FortiScan™ Vulnerability Management

Ordering Info		
Product	SKU	Description
FortiDB-400B	FDB-400B	FortiDB 400B. Includes license for 10 database instances.
	FC-10-D0400-135-02-DD	FortiDB Security Service (DBS)
FortiDB-1000C	FDB-1000C-E07S	FortiDB-1000C, includes license for 30 database instances, 4 10/100/1000 ports, 1TB HDD.
	FC-10-D1001-135-02-DD	FortiDB Security Service (DBS)
FortiDB-2000B	FDB-2000B-EMS01	FortiDB 2000B, Includes license for 60 database instances.
	FC-10-D2000-135-02-DD	FortiDB Security Service (DBS)

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispy, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and repair" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.



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

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
300 Beach Road 20-01 The Concourse
Singapore 199555
Tel: +65-6513-3730
Fax: +65-6223-6784

Copyright© 2011 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, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, 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.