



FortiDB™
Database Security and Compliance



FortiDB

FortiDB 500D, 1000D and 3000D

Database Security and Compliance

Discovery and Vulnerability Management — Database and sensitive data discovery, vulnerability management

Database Activity Monitoring and Audit — Both for privileged users and application users

Policy-based Intrusion Protection — Flexible framework to stop malicious transactions

User Access Management — Privilege summary and change monitoring

Database Risk Management and Compliance — For risk mitigation 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), audit 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 Security and Compliance

- Identifies and reports on confidential data access; aids in PCI-DSS, SOX and other regulations
- Periodic scan of every database in your network
- Built-in policies for database transactions and regulations such as SOX, PCI
- Policy-based Intrusion Protection
- Flexible deployment and centralized web-based management
- Flexible audit data collection methods — native auditing, network sniffer or lightweight agents
- Independent and secure audit storage
- Comprehensive audit/compliance reports
- Tight integration with ArcSight SIEM



HIGHLIGHTS AND DEPLOYMENT

Comprehensive Monitoring and Protection

FortiDB enforces acceptable use policies and alerts on database security threats. It continuously monitors all access to personally identifiable data (PID), financial data and other sensitive data types residing in your databases. Additionally, there is an option to block suspicious transactions, utilizing the same policies which were configured for alerting. FortiDB's full-featured monitoring and auditing technology manages critical policy issues such as change control, internal controls, privileged user monitoring, and privacy protection as well. Its change control features keep track of all changes related to database structures and users. The user privilege change monitoring function provides data for user access management and integration.

Granular Discovery and Vulnerability Management

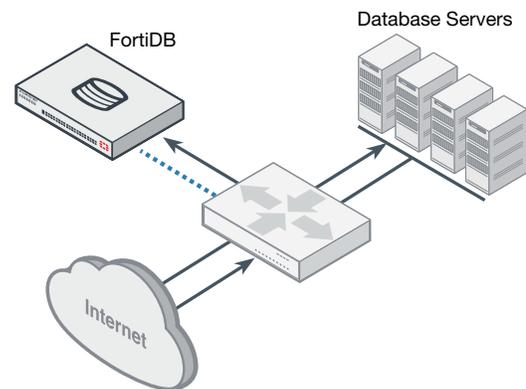
FortiDB provides Database and Sensitive Data Discovery functions. The Vulnerability Management function automatically detects new security weaknesses, policy noncompliance. FortiDB appliances and software ship with hundreds of preconfigured policies that address industry and governmental requirements, 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.

Accelerate Deployment and Lower Costs

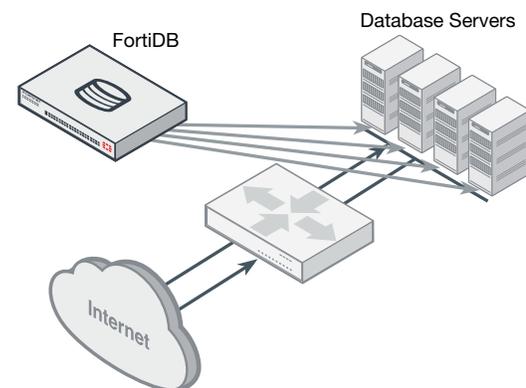
Flexible data collection methods ensure easy deployments even in complex environments. Native audit provides completeness and accuracy of audit data for both host based and remote connections. There is an agent based and a sniffer based option for audit data collection which does not require the native audit to be turned on.

The other area which can significantly decrease the complexity of the deployments is the ease of configuration. Besides the hundreds of predefined policies, there is an automatic policy generation function in FortiDB which streamlines the entire configuration process. Ultimately the two factors described above translate into quick deployments and lower costs.

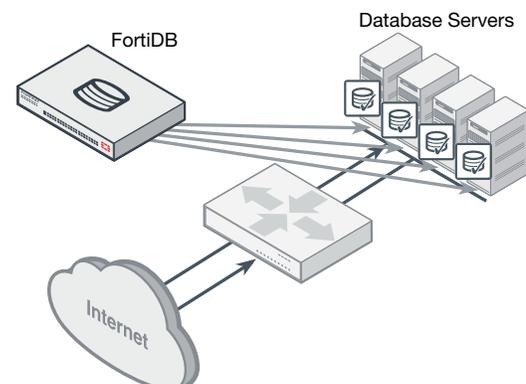
- Network Sniffer
 - No impact on the server
 - Zero network latency
 - Transparent to infrastructure



- Native Audit
 - Selective audit, only 3–4% performance impact
 - Does not require agents
 - Captures 100% of events



- Network Agents
 - 2–3% performance impact on the server (not the DB)
 - Agents send information back to FortiDB appliances



FEATURES

Best-In-Class Discovery and Assessment

- **Data and Database Discovery**
Besides the basic database discovery, FortiDB can also discover sensitive data such as credit card numbers, Social Security numbers etc. The results can be used for configuring policies to monitor sensitive data access.
- **Vulnerability Management**
Out-of-the-box policies facilitate immediate results. The policies are updated by FortiGuard, and can also be customized. They contain mappings to PCI, CIS and CVE numbers. Remediation advice provides an easy way to manage vulnerabilities.
- **Privilege Review**
The results of the privilege review can be used to establish a more secure role and access right setting in the database.
- **Profiling**
This function creates a user behavior model at the database level, at the individual user or table level. The results can be used to configure policies more accurately to identify suspicious access patterns.

Streamlined Policy/Control Configuration

- **Automated Policy Generation**
FortiDB can generate User, Session or Table access policies based on transactional data collected over a period of time. These policies then can be applied across multiple databases through the enterprise.
- **Out-of-the-box DDL, DCL, SOX, PCI Policies**
Most policies such as Data Definition Language (DDL), Data Control Language (DCL) and Compliance (SOX, PCI) are out-of-the-box in FortiDB. This facilitates quick configuration and deployment.
- **Privileged User Monitoring Policies**
For privileged user monitoring/audit, there is a quick setup process where the available usernames will be presented directly from the database. Alternatively, the automated policy generation function can be used.
- **Sensitive Data Access Monitoring**
Similar to the privileged user monitoring, tables and columns for monitoring can also be selected directly from the database. It is also recommended to run the sensitive data discovery, so the results can be turned into policies for data access. Alternatively, the automated policy generation function can be used.
- **Activity Audit Policies**
Besides the security focused alert policies, audit policies can also be defined in FortiDB, with the main purpose of auditing specific users or objects

Flexible Monitoring/Audit and Protection Capabilities

- **Privileged User and Application User Monitoring**
FortiDB can monitor privileged and application users. Both users can be specified during the configuration process. In some cases, a short research is recommended to identify the specific attributes of the two user types.
- **Configurable Real-time Alerts/Full Event Details**
Real-time alerts contain all the attributes which can uniquely identify transactions/users.
- **Separation of Duties**
There is a built-in role-based access management system in FortiDB. It is augmented by an asset-based model, where FortiDB users can be associated with certain groups of databases.
- **Policy-based Intrusion Prevention**
FortiDB can be configured to block suspicious transactions, utilizing the same policies which were created for alerting.
- **User Access Management and Integration**
Access levels in the database can be monitored for changes utilizing the predefined DCL alert policy group. Based on the results, access levels and roles can be adjusted. This information can also be sent to other access management systems for integration.

Reporting and Compliance Automation

- **Automated Compliance Reports/Integrated Compliance Frameworks**
In addition to the predefined compliance policies, FortiDB also provides the corresponding predefined compliance reports for SOX and PCI. This makes the configuration process quick and efficient.
- **Reports with Detailed Drilldowns**
Reports contain detailed information for more detailed analysis.
- **Predefined and Custom Reports**
There are multiple predefined reports for Vulnerability Management, Database Activity Monitoring and Compliance. Additionally, there are custom reports to meet specific reporting requirements.
- **Integration with SIEM**
FortiDB supports SYSLOG format which is common for SEIM tools. Additionally, there is a specific integration package for ArcSight.

Flexible Deployment Options

- **Appliance and Software**
FortiDB can be deployed as an appliance or as software. This makes the deployment process easier, especially in larger enterprises and virtualized environments.
- **Multiple Data Collection Methods**
All mainstream data collection methods are supported in FortiDB. Different data collection methods can be used for different databases on the same appliance or on the same software/VM instance.

FEATURES

The screenshot displays two main sections of the FortiDB interface. On the left is a navigation sidebar with categories like System, Administration, Target Database Server, Policy, Vulnerability Assessment, DB Activity Monitoring, and Report. The main content area is split into two views:

- Activity Profiling:** Shows a table of database activity for 'oracle_1fg2_10.101.0.50'. The table includes columns for Source IP (10.101.0.1), DB Instance (foundm-229bit), Pending Application (SQL Developer), DB User (xiangfan), and Session Count (1). Below this is a detailed table of database operations:

Table Name	Select	Update	Insert	Delete	Create	Alter	Drop	Trunc	Grant	Revoke
oracle.SYSTEM.student	0	0	0	1	0	1	0	0	0	0
oracle.SYSTEM.v_at	8	0	0	0	1	1	1	0	0	0
oracle.aos08.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.lab_test_dsl_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.lab_test_dsl	0	0	0	0	1	4	1	0	2	2
- Dashboard:** Provides a high-level overview of system health and security. It includes:
 - Target Database Server:** 9 defined, 9 complete, 0 incomplete.
 - Policy:** 655/45 total policies, 651 pre-defined, 4 user-defined.
 - Vulnerability Assessment:** 7 defined, 0 running, 133 runs, 196 vulnerabilities found, 47 informational results, 45 checks passed.
 - VA Vulnerabilities:** Two pie charts showing severity (Critical: 16, Major: 13, Minor: 8, Cosmetic: 1) and classification (Host System: 2, DB Server: 14, Privilege: 7, Password: 10, Configuration: 14, Unaffected: 9).
 - DB Activity Monitoring:** 9 target allow monitors, 2 currently monitoring, 10 alerts grouped.
 - Recent DAM Alerts:** A line graph showing alert trends from 09/08 to 15/08.

Activity Profiling – FortiDB automatically generates user activity baselines for easy policy configuration.

Dashboard – The FortiDB dashboard displays essential Vulnerability Assessment and Database Activity Monitoring/Audit information.

The screenshot shows the Alerts Summary and Alerts Analysis sections. The Alerts Summary view includes:

- Alerts Summary:** Total Alerts: 640717, Today: 30072, Recent 7 Days: 640717, Recent 30 Days: 640717, Recent 90 Days: 640717, Recent 12 Months: 640717.
- DB Activity Monitoring:** Target Allow Monitor: 9, Currently Monitoring: 2, Alerts Grouping: 10, Grouping Scheduled: 0.
- Recent Alerts Graphs:** Three line graphs showing alert trends for 'Recent 7 Days', 'Recent 30 Days', and 'Recent 90 Days'.
- Alerts Analysis:**
 - By Severity:** Informational: 26205 (0.04%).
 - By Policy:** My Alert user Policy (12390), Export-userPolicy (10403), My Alert table Policy (810), My Alert table column Policy (810), My Alert session Policy (892), Tables (408), Table Privileges (270), Tablespaces (270), vfan-sessionPolicy (264), System Privileges (33), sessionPolicy (33), 4.2.1-userPolicy (10), Export-tablePolicy (4), 4.2.1-sessionPolicy (3), Report-tableColumnPolicy (1).
 - By Action:** DB Action (21683), SELECT (1002), LOGON (596).

Alert Summary – High level overview of alerts and trends.

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

FEATURES

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

SPECIFICATIONS

	FORTIDB 500D	FORTIDB 1000D	FORTIDB 3000D
Hardware			
Security Hardened Platform	Yes	Yes	Yes
Number of Licensed Database Instances	15	30	90
Total Interfaces	4x GE RJ45, 4x SFP	6x GE RJ45, 2x SFP	4x GE, 2x GE SFP
Number of Hard Drives	2x 2 TB	2x 2 TB	2
Total Hard Drive Capacity	4 TB Raw, 2 TB RAID1	4 TB Raw, 2 TB RAID1	4 TB (2x 2 TB)
Storage Key (Boot Image)	2 GB	2 GB	2 GB
Redundant Hot Swappable Power Supplies	Optional	Yes	Yes
Hardware Form Factor	1 RU	2 RU	2 RU
Dimensions			
Height x Width x Length (inches)	1.7 x 17.2 x 16.4	3.5 x 17.2 x 14.5	3.4 x 20 x 29.7
Height x Width x Length (mm)	44 x 438 x 416	88 x 438 x 368	87 x 482 x 755
Weight	23 lbs (10.5 kg)	27.6 lbs (12.5 kg)	71.5 lbs (32.5 kg)
Environment			
AC Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz, 10 Amp (Maximum)
Power Consumption (Average)	135 W	115 W	317 W
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Humidity	5–95% non-condensing	5–95% non-condensing	20–90% non-condensing
Compliance			
	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE, BSMI, KC, GOST
Supported Platforms			
Database	DB2 UDB V8 (VA only), DB2 UDB V9.x (VA only), DB2 UDB V9.1/V9.5/V9.7; MS SQL Server 2000/2005/2008/2008R2, MS SQL Server 2012; MySQL 5.1/5.5; Oracle 9i/10gR1/10gR2/11g; Sybase ASE 12.5 (sniffer only) 15.0.2/15.02/15.5/15.7 (MDA only)		
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, 9; Firefox 3, 4, 5		

ORDER INFORMATION

Product	SKU	Description
FortiDB 500D	FDB-500D	FortiDB 500D, includes license for 15 database instances.
FortiDB 1000D	FDB-1000D	FortiDB 1000D Database Security and Compliance Appliance, includes license for 30 database instances, 6x GE RJ45 ports, 2x SFP ports, 2x 2 TB storage.
FortiDB 3000D	FDB-3000D	FortiDB 3000D, includes license for 90 database instances, 4x 10/100/1000 RJ45 ports, 2x GE SFP ports, 2x 2 TB HDD storage.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480