

## 7 @ 53

4 V @ R K U S P S M V T f @ 0  
W 5 2 5 F U V h c d

5 R P W e

## 5 R P U S R U / Z X V M V f @ A J j @ ^ a j R T V R U V @ X

### < h M X 6 0 h v c

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 vulnerability assessment capabilities.

### D J f z \_ o v e s \_ R \_ Z O M f @ R R W ^ V @

The FortiDB Family of products provide centrally managed, enterprise-scale, database hardening features with fast, comprehensive policy compliance 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. Automatic database discovery quickly finds all databases on the network, across subnet and WAN boundaries. 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.

< j @ J f z _ o v e s _ R _ Z O M f @ R R W ^ V @	
• Automatic Database Discovery	High-performance scans quickly find all databases on the network and across WAN and subnet boundaries – even on irregular ports.
• Accelerated Security and Compliance Best Practices (PCI, SOX, HIPAA)	Automatic updates to latest regulatory / industry best practices add to hundreds of pre-populated security and compliance policies.
• Centralized Policy Management	Centralized web-based access allows DBAs to more quickly identify and react to database security threats across the network.
• Business-Driven Assessments with Flexible Sets of Policies	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.
• Standardized Compliance Reports with Trend Analysis	Standardized, exportable reports customizable with company branding are designed out-of-the-box to support compliance programs, with graphic trend analysis to spot and isolate patterns.
• Enterprise Scalability	Supports flexible deployments across the network of up to 30 databases per appliance for consistent enterprise-wide policy enforcement.
• Built to leverage the Fortinet Product Portfolio	Designed with a familiar Fortinet interface style similar to that utilized across all supporting Fortinet application product lines, including FortiMail and FortiAnalyzer.



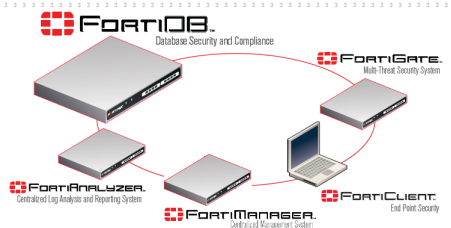
FortiDB-1000B



Fortinet Database Security Software

### = h ^ a R i e e j a t d e v h v a z o E 4 @

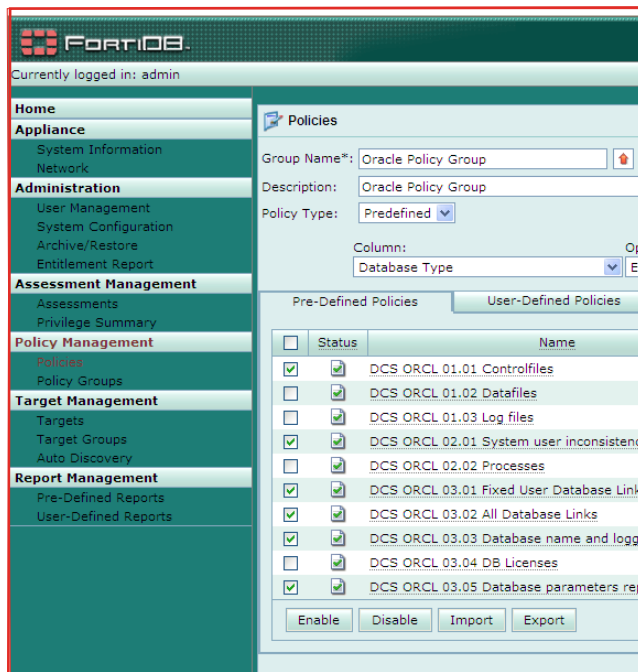
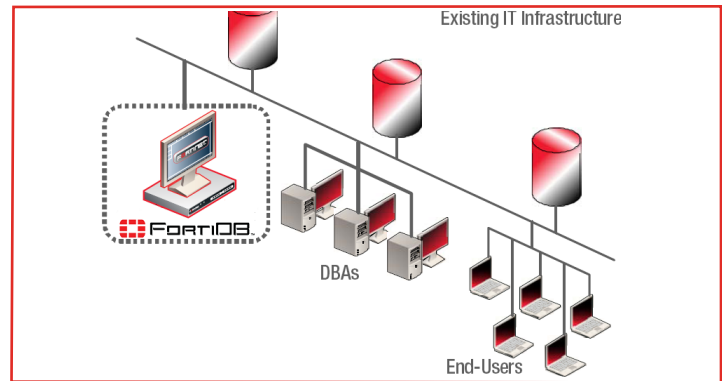
Failing to keep up with today's regulations for data security can be cost prohibitive. FortiDB simplifies the process with regular policy and signature updates via XML, and current industry leading remediation advice that strengthens the integrity and security of databases – mitigating internal threats, 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.



## 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

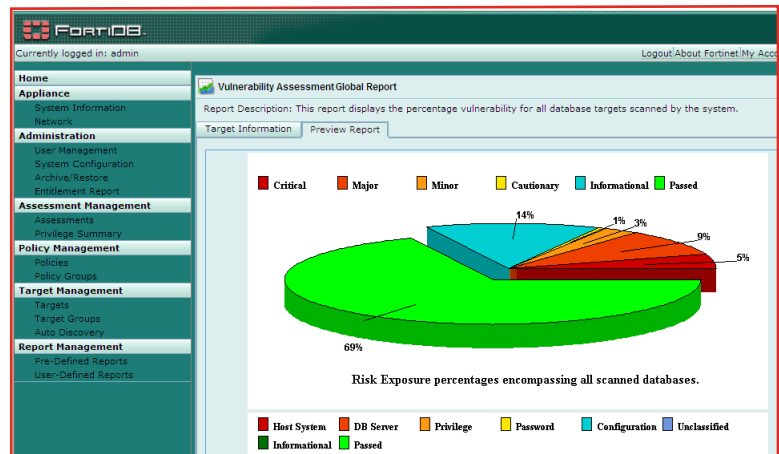
New regulatory, compliance and legal mandates largely in response to headline-grabbing security breaches and accounting scandals require businesses to not only understand database events, but also proactively implement and enforce database security policy. Selecting a compliance solution that keeps up 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.





Feature	FortiDB-1000B
Security Hardened Platform.....	Yes .....
Number of Licensed Database Instances.....	30.....
10/100/1000 Ethernet.....	4.....
RAM .....	2.0 GB .....
Number of Hard Drives .....	1.....
Total Hard Drive Capacity.....	250.0 GB (1TB option).....
USB Storage key (boot image).....	1.0 GB .....
RAID Storage Management.....	No .....
Redundant Hot Swap Power Supplies.....	No .....
Dimensions (H, W, L) .....	1.7 x 16.7 x 30.4 in... .. (4.3 x 42.6 x 77.2 cm) .....
Weight.....	35.8 lbs (16.3 kg) .....
Rack Mountable.....	Yes .....
Input Voltage-Current.....	100-120V-10A / 200-240V-4.8A.....
Auto-switching universal .....	110/220 Volts.....
Average Power Consumption .....	275.4 Watts.....
Maximum Power Consumption .....	1200 Watts .....
Operating Temperature .....	50 to 95 deg F (10 to 35 deg C).....
Storage Temperature .....	-40 to 149 deg F (-40 to 65 deg C).....
Humidity .....	5 to 95% non-condensing (twmax=38C) .....
Regulatory .....	FCC Class A Part 15 / CE Mark .....
Database support.....	DB2 UDB V8, DB2 UDB V9; Microsoft SQL Server 2000, Microsoft SQL Server 2005; Oracle 8.1.6, Oracle 8.1.7.4,..... Oracle 9.2.0.x, Oracle 10.2.0.x, Oracle 11.1.0.x; Sybase ASE 12.5.4, Sybase ASE 15.0.2 .....
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 2.0.0.x.....

Feature	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; .....
Database support.....	DB2 UDB V8, DB2 UDB V9; Microsoft SQL Server 2000, Microsoft SQL Server 2005; Oracle 8.1.6, Oracle 8.1.7.4,..... Oracle 9.2.0.x, Oracle 10.2.0.x, Oracle 11.1.0.x; Sybase ASE 12.5.4, Sybase ASE 15.0.2 .....
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 2.0.0.x.....

**76533** ^aR IVA IJ obvtr V @R L0Va cZ X0VRe dD  
 76533fa ca @B VVJ hZXT ^aR IVA IJ obvtr V @R L0Va cZ X0VRe dD-

- 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, GBLA, 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 interface**

The Simple Network Management Protocol (SNMP) interface 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, specific 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.

