



Is your data **really** safe?

**FORTINET.**





# ARE YOUR INTERNAL SYSTEMS REALLY KEEPING DATA SAFE?

Information theft and fraud has enriched thieves and bruised company reputations. Attackers frequently target the holy grail of critical information – the database.

Fortinet provides a simple, fast way to harden all your databases against attack. We provide best practice policies to fix problems before data is compromised, misused, or stolen. Our solutions easily adapt to your environment, offering custom security policies and reports for business-specific issues.

So, how are *you* keeping data safe?

### ***Vulnerability Assessment – the Essential Starting Point***

Vulnerability Assessment (VA) is the automated discovery and periodic examination of databases for known weaknesses that enable unauthorized access to data, settings, and configurations. Just the type of solution you need to keep *your* data safe.

Fortinet addresses three key VA areas:

- Data Security
- Resource Efficiency
- Business Continuity



## FORTINET SECURES YOUR DATA

### ***Auditor-friendly Design***

Auditors now expect consistent, verifiable controls that ensure continuity of security policies – both industry standard and internal best practice – across entire organizations. These include:

- Regulatory requirements for public companies
- Financial best practices for private companies
- Collateral requirements for inter-company business

Fortinet assists auditors in the design of pre-packaged reports, with the specific inclusion of:

- CobiT references
- Control assertions
- Sign-off fields

In addition, there is implicit separation of duties – policy creation, policy management, and compliance review are all conducted independently.

### ***Custom Controls***

Custom reporting allows the modification of existing reports and creation of new reports to meet your specific regulatory, compliance, or enterprise security requirements.

Out-of-the-box policies can be easily edited to adjust risk level, criticality, action, and remediation advice. Proprietary best practices can also be quickly captured as custom policies; and the frequency of vulnerability scans can be set according to need; for example, critical databases can be assigned a higher frequency.

### ***Verification & Assurance***

In practice, existing scripts are often irregularly applied and inconsistent across business units. Fortinet solves this issue by automatically maintaining a history of all activities.

Finally, data can be exported in encrypted format to support independent audit verification.



## IMPROVE EFFICIENCY

The popular belief is that controls are difficult and time consuming to build, expensive to implement and maintain.

Excessive resource costs can be incurred through:

- Script development and maintenance
- Keeping up-to-date on the latest threats for all databases and database versions
- Manual reporting

Consistent application of internal scripts is often difficult, product system issues out-prioritize causing inconsistency, and differences between groups interpretations. Without on-going maintenance, custom infrastructures for monitoring and alerting to quickly identify and resolve vulnerabilities disintegrate.

### ***Discovery & Automation***

Fortinet auto-discovery eliminates the time-consuming and error prone manual work of identifying all database servers and database instances.

- Call-Level Interface (CLI) for script-based automation
- SNMP for integration with pre-existing ticket management, existing patch management solutions, trouble ticketing systems, systems and network management platforms, etc

### ***Seamless Integration***

Fortinet features automation and integration with existing patch management solutions, trouble ticketing systems, systems and network management platforms, or any third party solution through a CLI and SNMP.

Real-time alerts can be received through email, pagers, etc, and there is support for a wide variety of databases, including Oracle, Microsoft, IBM DB2 UDB and Sybase.

### ***Centralized Management***

Database servers can be managed across LANs and WANs from one location, and policy changes made. Upgrade policies need only be applied once – they then automatically migrate to all servers.

- Regular policy updates provide industry standard best practices
- 48-hour turnaround upon publication of critical database or database-related OS-level vulnerabilities

Role separation is provided. For example, some users can run scans, others can only see them.





## REDUCED RISK, REDUCED COST

Every application, web or enterprise, uses a database that should be held to equivalent security standards. Most mission critical applications require reliable 24x7 access to the database.

The core issue here is that perimeter security is insufficient – it misses key activities that are database-centric.

The corporate liability associated with these risks is extremely high:

- Cost of application black- or brown-outs
- Cost of corrupted data or compromised configurations
- Cost in dissatisfaction and lost customers
- Cost of litigation, fines and defamed reputation

### ***Find/Fix Flaws Fast***

Fortinet's solutions are specifically designed to maintain your day-to-day business efficiency:

- Installs in minutes
- Out-of-the-box reporting finds flaws fast
- Remediation advice enables immediate resolution of vulnerability issues

### ***Enterprise Class***

Fortinet uses enterprise class components such as Windows, Linux, Solaris, Oracle, DB2, MS SQL Server, Websphere and Tomcat/Apache.

Efficient vulnerability scans allow scalability to support thousands of databases, even ones distributed geographically across the wide area. All this with just a single instance of Fortinet.

And for complete control, a browser-based interface provides a single view of your entire enterprise as well as administration from anywhere.



## KEY COMPONENTS TO DATA GOVERNANCE

### **Auto-Discovery**

- Quickly discovers all database types
- Finds databases on any ports
- Works in LAN and WAN environments
- Discovery of sensitive data

### **Agent-less Deployment**

- Connects directly to the database through normal connection
- Non-invasive and does not affect database performance
- Does not require administrator privileges

### **Configuration Management**

- Assess existing configuration settings
- Remediation advise for secure configuration settings

- Integration with other configuration management tools

### **Up-to-Date Security Measures**

- Prevent hackers from exploiting vulnerabilities
- Identify correct patches and verify that small changes are not missed
- Our research team keeps you up to date

### **Full Database Coverage**

- Policies for all major database providers
- Support for current production and legacy database versions

### **Hundreds of Best Practices**

- Years of industry best security practices pre-bundled
- Provides expert level analysis and remediation tips

- Custom policy capability
- Lowers risk of human error

### **Automated Reporting**

- Scans and reports can be scheduled to ensure timeliness
- All alerts can be individually provided to other services
- All reports can be placed into different formats, such as PDF, HTML and text files

### **Central Policy Management**

- Single policy repository allows for consistent policy application
- Web-based interface provides 'manage anywhere' capability
- Maintains scan history for trend analysis





**YOUR TIME COULD BE  
RUNNING OUT.  
CONTACT FORTINET AND  
KEEP YOUR DATA SAFE.**

## ABOUT FORTINET

Fortinet, Inc.'s award-winning software is **Keeping Data Safe** for companies around the world. From hardening databases against attacks to real-time activity monitoring, Fortinet is the solution to enterprise compliance and database security needs.

For more information please call

AMER +1-408-235-7700

EMEA +33-4-8987-0510

APAC +65-6549-7050

click [www.fortinet.com](http://www.fortinet.com)

or visit 1090 Kifer Road, Sunnyvale, CA 94086, USA

Fortinet and the Fortinet logo are trademarks of Fortinet, Inc.  
All rights reserved. Any unauthorized use or reproduction of the  
Fortinet logo is prohibited.  
© 2008 Fortinet, Inc.

**FORTINET.**

Design by [www.rightangle.co.uk](http://www.rightangle.co.uk)

