

PCI Compliance with Enzo DBMS Firewall

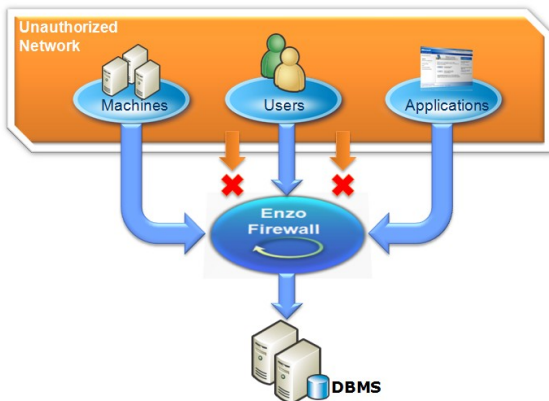
Overview

PCI compliance imposes strong security requirements for organizations dealing with Credit Card data. Through real-time **DBMS Authentication, Authorization and Access Control (AAA)** Enzo Firewall simplifies PCI compliance initiatives.

Strong AAA

Central to all compliance initiatives, including PCI, corporations need to implement strong DBMS AAA.

Enzo Firewall gives corporations **fine-grained DBMS AAA controls** for stronger database security, including **real-time** DBMS connection policies controlling who, what, when and where.



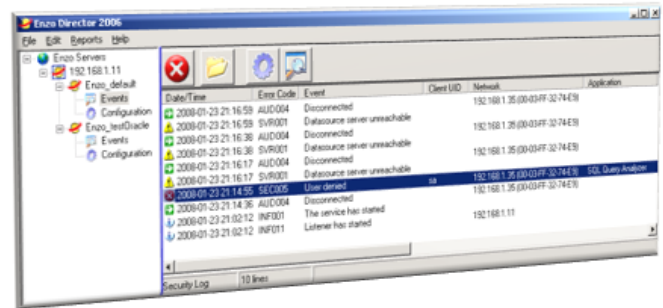
Network Segmentation/IPS

With Enzo Firewall, corporations can also **segment** DBMS Networks by blocking connectivity from weak network zones, such as DMZ and Wireless locations.

With its Security by Default configuration **Enzo Firewall hides database servers** except from authorized locations. This can help **reduce the network footprint** that corporations need to include for their PCI initiatives.

Unauthorized Access Detection

The ability to detect unauthorized activity is another important aspect of PCI. With Enzo Firewall, corporations can be alerted of failed login attempts in real-time. Enzo Firewall also provides reports that show the **originating IP address** of the failed login attempts to assist with forensics analysis.



Enzo Firewall provides three kinds of real-time alerts: **SMTP** (email), **Syslog** and **ODBC**.

Prevent Hacking

Corporations can take advantage of Enzo's security features to minimize hacking such as:

- Prevent use of backdoor accounts
- Block database discovery activity
- Control use of shared accounts

Specifications

- Windows XP, Windows 2000 or higher
- 256MB of RAM minimum
- 100MB Disk space (+ log space)
- Supports SQL Server 2000 or higher and Oracle 9i and 10g