Imperva SecureSphere Database Security

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Imperva SecureSphere Database Security

Read 9 reviews of Imperva SecureSphere Database Security

Review by a Real User

Verified by IT Central Station

Officer- Informations Systems Security Audit
at a government with 501-1,000 employees

it_user254976

VALUABLE FEATURES

Database activity monitoring Web application firewall

IMPROVEMENTS TO MY ORGANIZATION

This product has limited attacks to the core tax collection application. It also provides audit logs for changes to the database and gives user account details.

ROOM FOR IMPROVEMENT

None so far.

USE OF SOLUTION

I've used it for over two years.

DEPLOYMENT ISSUES

I was not around during the implementation, but reports do not show any issues noted.

STABILITY ISSUES

None so far.

SCALABILITY ISSUES

None so far. Our solution has not had bottlenecks so far

Imperva SecureSphere Database Security

Read 9 reviews of Imperva SecureSphere Database Security

CUSTOMER SERVICE AND TECHNICAL SUPPORT

Customer Service: Customer service has always been available. Technical Support: Technical support is rated highly.

PREVIOUS SOLUTIONS

Only a firewall was in place before. WAF was needed for web application specific protection as firewalls are not the best solution.

INITIAL SETUP

No issues noted in the implementation reports.

IMPLEMENTATION TEAM

A third party vendor was used to implement the product and to get the IT security staff trained.

ROI

We have had a high **ROI** with this product.

PRICING, SETUP COST AND LICENSING

Budget for licenses in synch with your financial years, and it's best to have licenses covering over a year so that planning for procurement of new licenses is done earlier. Of course, if you operate in AWS cloud, its much easier to justify as you can pay for three or more years at once.

OTHER SOLUTIONS CONSIDERED

I am not privy to procurement details, but we use Gartner as a source. Imperva is the sole leader in its field.

OTHER ADVICE

Implement this product across all systems running applications as access to one unprotected system can be elevated to a protected one. Also, have reports produced frequently using the tools available in the system and analyze them to know and investigate the sources of attacks the WAF has blocked. That's because they could be internal indicating a compromise or a malicious user within. Ensure that your SharePoint environment is also protected as though it may be internal, attacks can be directed at it.

Read 9 reviews of Imperva SecureSphere Database Security