



CMP

United Business Media

# InformationWeek

SEPT. 24, 2007

DEFINING THE BUSINESS VALUE OF TECHNOLOGY

For IT By IT

## Smokin' Databases



By John H. Sawyer

Today's ace attackers are gunning for fortune, not fame, and they know that the big score lies at the end of a SQL query. Got protection?

informationweek.com

**W**HEN A WEB SERVER ATTACK exposed Second Life customer data last September, Linden Lab invalidated all user passwords and announced that one lowly SQL injection flaw had enabled attackers to run arbitrary SQL commands on a back-end database. The company admitted that 650,000 names along with contact information, encrypted passwords, and payment data had been compromised.

Fast forward to May, when University of Missouri employees probably wished they were in some alternate universe. IT staff noticed abnormal application behavior on May 3 and the next day discovered a mother lode of errors. One vulnerability was in a Web page used to check the status of help desk issues, and by exploiting a SQL injection flaw, an attacker was able to retrieve names and Social Security numbers the old-fashioned way—one record at a time, using tens of thousands of Web requests.

By the time IT realized what was happening, sensitive data on 22,396 people was long gone.

### YOUR MONEY AND YOUR DATA

It's no coincidence that over the past year an increasing number of security breaches have been the result of database compromises, rather than pilfered laptops. Steal a PC from a car and you might get nothing but some hardware and an MP3 collection. Infiltrate a database of customer information and the possibilities are endless. And this trend will only continue as more companies deploy data-rich online services needing database back ends.

In the case of Second Life, attackers mined personal information on thousands of users who might have ended up the focus of highly targeted phishing scams. For the University of Missouri, affected employees must worry about identity theft because of one insecure Web application and an old database still left in service.

Sure, it would be ideal if secure programming techniques were always followed when developing Web applications. But let's face it, basing your data security strategy on developers producing bulletproof apps is like going to a shootout with one round in your magazine.

A better idea? If Linden Lab and UM had database extrusion prevention systems de-

Sept. 24, 2007

played at the time of the compromises, these breaches could have been prevented. The offerings we reviewed in our DBEP Rolling Review can keep abnormally large numbers of records from being returned, as in the Linden Lab compromise, and block the SQL injection attacks seen in the UM hack.

In the arsenal of IT defenses, DBEP systems have a slight advantage over standard data leakage protection products that sit at the network perimeter or run as endpoint agents in that they can be placed directly in front of your databases. They see traffic before an attacker can obfuscate, transform, or encrypt data to evade detection. With data leak prevention, an attacker can avoid discovery if he gains a level of control over the data before it's shuttled through the network.

Enterprises worried about exposure through attacks against Web servers with database back ends, the database servers themselves, or via misuse by authorized users have protection

options—we were generally pleased with the products we reviewed, with only a couple of exceptions. These products aren't one-size-fits-all, but any of the five could have prevented a good number of the breaches that are currently making news.

## WILD CARDS

We put five DBEP systems to the test in our University of Florida Real-World Labs. Crossroads Systems, Guardium, Imperva, and RippleTech sent us appliances, while Pyn Logic submitted software. We also invited Application Security, IPLocks, Symantec, Tizor Systems, and Transparency Software. Symantec declined. Application Security and Transparency Software didn't have their latest revisions ready within our testing window. The others never responded.

When we started testing, we weren't entirely sure what to expect, but we knew exactly what we were looking for: ease of installation and configuration, a breadth of database support, good visibility into database activity, detection and no-

Real-World Analyst Assessment: Database Extrusion Prevention					
UNACCEPTABLE ← ● — ● — ● — ● — ● → IDEAL					
	Crossroads	Guardium	Imperva	Pyn Logic	RippleTech
<b>Shortlist</b> ✓ <b>Editor's Choice</b> ☆ <b>Best Value</b> \$	✓	✓	✓ ☆		✓ \$
<b>Ease</b> of installation and configuration	●	●	●	●	●
<b>Breadth</b> of database support	●	●	●	●	●
<b>Visibility</b> and understanding of database activity	●	●	●	●	●
<b>Detection</b> and notification or blocking attacks	●	●	●	●	●
<b>Overall</b> features	●	●	●	●	●
<b>Price</b>	●	●	●	●	●
<b>Crossroads Systems DBProtector:</b> Even though DBProtector doesn't have all the features found in Imperva's and Guardium's products—and yet costs the same—the company is off to a great start with usability and visibility into database operations. Right now, enterprises will be better off choosing Imperva or Guardium based on features and price, but we wouldn't be surprised to see Crossroads close the gap over the next six to 12 months.					
<b>Guardium SQL Guard:</b> SQL Guard is a great product and a close second to Imperva. Reporting is top-notch, and the appliance's ability to automate practically everything will make it a popular choice for busy security administrators. Enterprises of any size will find SQL Guard a solid fit.					
<b>Imperva SecureSphere Database Security Gateway:</b> Imperva's dynamic user profiling is almost reason enough to choose it. Other features, including stateful firewall, IPS, and database vulnerability assessment, are icing on the cake. The ability to manage all SecureSphere instances from one console makes it a good fit for any size enterprise.					
<b>Pyn Logic Enzo 2006:</b> Enzo 2006 does a good job of blocking access or allowing access based on who, what, where, and when. However, its architecture limits it to smaller companies that understand their database usage backward and forward.					
<b>RippleTech Informant:</b> While Informant doesn't have the capability to block traffic, it does a good job of reporting. The included metrics for monitoring database usage are second only to Imperva in sheer number and usefulness. Companies that don't need blocking features and want the best bang for the buck will like Informant. Its interface needs some work, though.					

tification or blocking of attacks, helpful features, and a reasonable price.

To be effective, DBEP systems must provide visibility into database activity, whether it occurs on the network between the database and application servers or locally on the database server. Rules can then be created to monitor for activities that indicate possible misuse or attack. After an activity is detected, it can be allowed, blocked, or recorded, or an alert can be sent out.

Up to this point, all the products we tested worked pretty much the same. It's the extras that separated the leaders from the rest.

We found it interesting that the top two vendors in our review, Guardium and Imperva, approach the problem of database extrusion differently. Imperva focuses heavily on network security, with features like a stateful firewall, intrusion prevention system signatures, and vulnerability scanning of the database server. Guardium, in contrast, concentrates more heavily on reporting. We found at least a dozen different ways to take data gathered during monitoring and turn it into automated audit statements and security assessments that report on the security of a database server based on generated alerts, not by testing the server directly.

Baselining database activity and creating related policies are a key differentiator for the appliances from Crossroads, Guardium, and Imperva. Each could monitor database activity and determine a base policy to fit the usage profile. Imperva stood out for its dynamic profiling, which monitored activity, created usage profiles, and then let those profiles dynamically update themselves by defining safe margins and hard limits. For any enterprise with large-scale database deployments, this is a welcome feature that will spare DBEP administrators from constantly having to update policies as user roles change over time.

Management was performed through a Web browser for all the products tested, except for Crossroads DBProtector,

which features a Java-based interface. We saw few usability issues in the Web interfaces, though it became obvious after testing with both Mozilla Firefox on Linux and Internet Explorer on Windows that they were built with IE in mind. Crossroads' Java interface is both pleasing to the eye and easy to navigate. For the Web-based offerings, Guardium's and Imperva's GUIs are well done, with Guardium's being slightly more polished.

## EDITOR'S CHOICE

Right from the start, Imperva SecureSphere Database Security Gateway impressed us with its plethora of features. Deployment options include both in-line and out-of-band monitoring via a switch's network monitoring port or network tap, with both options allowing blocking either by dropping traffic entirely when in-line or sending TCP reset packets when out-of-band. Only one other entry, Guardium SQL Guard, has the same blocking capability.

Unique to Imperva SecureSphere was the ability to scan the database server for vulnerabilities and act as an intrusion-prevention system. The gateway scans the database software and underlying operating system to find known vulnerabilities and weak security configurations that could allow the server to be compromised. Additionally, when deployed in-line, it can act as a stateful firewall and IPS with more than 2,500 signatures to prevent attacks such as protocol violations, SQL injection, and known worm activity. SecureSphere cost \$45,000 as tested and is our Editor's Choice for this Rolling Review series.

See our full reviews of Crossroads Systems DBProtector, Guardium SQL Guard, Imperva SecureSphere Database Security Gateway, Pyn Logic Enzo 2006, and RippleTech Informant at [nwc.com/rollingreviews/extrusion-prevention](http://nwc.com/rollingreviews/extrusion-prevention).

John H. Sawyer is a senior IT security engineer at the University of Florida and a GIAC certified firewall analyst, incident handler, and forensic analyst. Write to him at [jsawyer@nwc.com](mailto:jsawyer@nwc.com).



### BUILD IT RIGHT

Bake in security at the start, avoid pain later:  
[nwc.com/go/data-security-architect](http://nwc.com/go/data-security-architect)

### CAUTIONARY TALE

Was data on 6.3 million brokerage customers taken?  
[nwc.com/go/ameritrade](http://nwc.com/go/ameritrade)