White Paper

Application and Database Security with F5 BIG-IP ASM and IBM InfoSphere Guardium

Organizations need an end-to-end web application and database security solution to protect data, customers, and their businesses. The integrated solution from F5 and IBM provides improved protection against SQL injection attacks and correlated reporting for richer contextual information.

by David Holmes
Technical Marketing Manager

by Peter Silva
Technical Marketing Manager

Contents

Introduction

Information technology recognizes defense in depth as a best practice in system protection. Defense in depth fortifies infrastructure and systems with a layered security approach. Firewalls are stationed at the edge of the network and security mechanisms are usually deployed at every segment. If attackers circumvent the first layer, the next one should net them.

In IT, employing a defense in depth strategy involves redundancy: placing multiple iterations of a defensive mechanism in the path of an attacker. The muscle of a firewall is a critical defense component, but to achieve a truly secure system, fortification must also be based on context. A system with context takes into account the environment or conditions surrounding an event to make an informed decision about how to apply security. This is an especially important part of protecting a database.

Using these principles, F5 and IBM have extended their long partnership to offer enhanced security for web-based database applications. The integration between F5® BIG-IP® Application Security Manager™ (ASM) and IBM InfoSphere Guardium provides richer forensic information about application security and database attacks (such as SQL injection and other OWASP top 10 attacks) through correlated reporting.

Contextual Database Security

A database is the primary repository and retrieval mechanism for an enterprise's critical data—so protecting that database is crucial. As more application traffic moves over the web, sensitive data is exposed to new security vulnerabilities and attacks. Standalone technologies that protect against web or database attacks are available, but their disconnection from one another means they lack context. Organizations need an end-to-end web application and database security solution to protect their data, their customers, and ultimately their businesses.

SQL injection is an attack in which the attacker inserts malicious code into a string that is then passed on to the database for execution. This is usually accomplished by entering a SQL query or command script in a user input field, such as the password field. The attacker is essentially trying to bypass the application servers in order to manipulate the database directly. A successful attack could result in just unauthorized entry, or it could return the entire database containing user names, passwords, and other sensitive information. A typical database security solution,

End to end security

In the combined solution, BIG-IP ASM provides security data from the front-end of the application, while InfoSphere Guardium correlates that data with its own from the back-end database to provide the reporting and visibility that today's businesses need to stay secure.

which may protect against such an attack, does not have the visibility to gather information such as the attacker's host name, user name, client IP, and browser. While it can see that a particular SQL query is invalid, it cannot decipher who made the request.

A web application firewall (WAF), on the other hand, gathers user-side information so it can base policy decisions on the user's context. A WAF monitors every request and response from the browser to the web application and consults a policy to determine whether to allow the action and data. It uses information like user, session, cookie, and other contextual data to decide if the request is valid. WAFs are primarily focused on HTTP and HTTPS attacks and do a great job of thwarting that type of malicious traffic. They can also block most database-targeted attacks launched through a browser. However, given the complexity of detecting SQL injection attacks in the web application tier (i.e., lack of SQL-related context, understanding of SQL protocol) WAFs are not a foolproof SQL injection prevention solution. There is a chance of false positives or overlooked attacks.

The answer is a joint solution from F5 and IBM that links a web application firewall with a database security solution. The integration of F5 BIG-IP ASM and IBM InfoSphere Guardium offers the database protection that IBM is known for with the contextual intelligence that is baked into every F5 solution. BIG-IP ASM provides the data from the front-end of the application. InfoSphere Guardium correlates that data with its own from the back-end database to provide the reporting and visibility that today's businesses need to stay secure.

The power of BIG-IP ASM and InfoSphere Guardium working together is in the consolidated reporting of attacks and the ability to set policy at the web application layer, which is coordinated at the database layer. With F5 and IBM, an enterprise's database is protected by a layered, defense-in-depth architecture, backed with the contextual information required to make informed, intelligent decisions about database security incidents. It's a comprehensive approach that enables enterprises to adapt quickly to changing threats and provides the logging and reporting capabilities needed to meet auditing and compliance regulations.

Two-Tier, End-to-End Protection

The F5 and IBM partnership has a long history of producing integrated solutions. For example, BIG-IP ASM has long supported IBM's Security AppScan, formerly a Rational product that scans applications for vulnerabilities. BIG-IP ASM is an advanced WAF that provides comprehensive edge-of-network protection against a wide range of web-based attacks. It analyzes each HTTP/HTTPS request and blocks potential attacks before they reach the web application server. IBM InfoSphere Guardium is the first line of defense for databases, providing real-time monitoring of database activity on the network. Highly accurate, SQL grammar–based technology blocks unauthorized transactions, which helps prevent attacks from reaching the database. InfoSphere Guardium is deployed between the web application server and the database. It provides protection against attacks originating from inside or outside the network and works by analyzing the intent of the SQL statements sent to the database. It does not depend on recognizing the syntax of known security threats, and it can therefore block previously unseen attacks. It is easy to deploy, as it requires no changes to existing applications or databases.

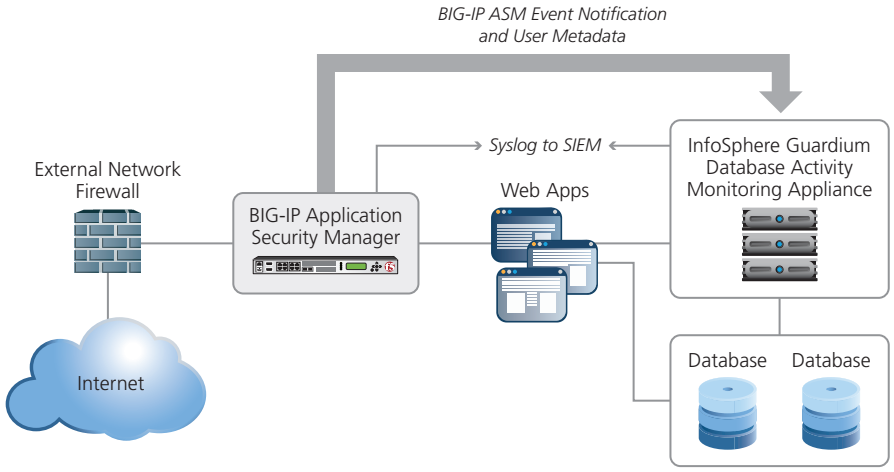
How BIG-IP ASM and InfoSphere Guardium Work Together

BIG-IP ASM and IBM InfoSphere Guardium work together on reporting breaches, preventing data leakage and providing auditors with the governance they need for compliance.

Working Together to Detect and Report Breaches

When threats to data are detected, the combined solution monitors, alerts, or blocks the threat, and the identity of the user is shared between BIG-IP ASM and InfoSphere Guardium. In the case of a malicious SQL injection, InfoSphere Guardium would block the injection instantly and log the action, but it can't determine who attempted the breach. BIG-IP ASM gathers the user name, client, browser, session information, time, cookies, URL, SQL statement, and so on. The IBM reporting engine then correlates the BIG-IP ASM data with its own and generates a report that there was an attempted breach, with the critical data needed to determine who caused the trigger. The triggered alerts and accompanying detailed reports provide immediate notification on the type and severity of a threat.

With two information sources, BIG-IP ASM and IBM InfoSphere Guardium, the resulting correlated data is richer, making policy creation more accurate and more granularly refined. With this level of detail, malicious or compromised users can be isolated, forced to re-authenticate, or prevented from accessing the application in real time. Subsequent attacks from the same user can be prevented, diverted, or rendered inert by the F5 and IBM solution.



BIG-IP ASM secures web traffic, and IBM InfoSphere Guardium secures database traffic. BIG-IP ASM passes user log-in information to InfoSphere Guardium. If a SQL injection takes place, BIG-IP ASM sends all context of the attack to InfoSphere Guardium. The user's identity can now be associated with the attack in reports, based on session and the BIG-IP ASM session cookie.

Figure 1: F5 BIG-IP ASM and IBM InfoSphere Guardium correlate and report on security events.

Combining to Prevent Data Leakage

In the unlikely event that information is compromised, BIG-IP ASM addresses the issue on the response. The Mask Data feature in BIG-IP ASM automatically scrubs sensitive data as it passes through to the user, preventing any data leakage.

For instance, if a malicious user circumvented the system and generated a request for credit card information from the database, BIG-IP ASM would either block that request or scrub the output by replacing the credit card number with asterisks.

Reporting Together to Gain Compliance

When used with the reporting tools of IBM InfoSphere Guardium, the data leakage prevention and breach detection features of BIG-IP ASM can be instrumental in gaining or maintaining regulatory compliance. Reporting and auditing are top criteria for many of the regulations in place today, including the standards of the Payment Card Industry (PCI), Health Insurance Portability and Accountability Act

(HIPAA), Sarbanes-Oxley Act (SOX). This solution can help ensure companies have the most detailed compliance information.

Finally, one of the most significant benefits of this solution is that it can protect any SQL-based database, including IBM DB2, MySQL, PostgreSQL, Hadoop, Netezza, Oracle Database, Microsoft SQL Server, and Sybase databases.

Conclusion

The integration of F5 BIG-IP ASM and IBM InfoSphere Guardium enhances security for web-based database applications. Combined, the two solutions give enterprises the layered protection that security professionals recognize as a best practice, plus the contextual information needed to make intelligent decisions about what action to take when an attack is attempted. The integration between solutions provides F5 customers with improved SQL injection protection and IBM database customers with correlated reporting for richer forensic information on SQL injection attacks.

The F5 and IBM partnership has developed solutions that help organizations create agile IT infrastructures that align with their business demands. With F5 and IBM, enterprises' sensitive database information is always secure, available, and delivered quickly.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com