F5 PARTNERSHIP SOLUTION GUIDE

F5 and IBM Software

Security Solutions

Protect people, data, applications, and infrastructure

WHAT'S INSIDE

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

ICSA labs CERTIFIED SSL VPN

Business Partner IBM™

Ready for Security Intelligence

Enhance Access While Protecting Against Security Threats with F5 and IBM Unified Security Solutions

Keeping data center services secure, fast, and available is crucial for business success. Security breaches and multi-layer cyber attacks can result in lost productivity, missed opportunities, and higher costs. They can also damage the organization's reputation and deteriorate customer trust.

F5 and IBM Security Solutions enable, simplify, and accelerate access for your people while protecting the organization's data, securing applications, and enabling holistic management of security intelligence for the data center infrastructure. Your organization gains the security it needs and users will enjoy the access they demand.

Secure and accelerate access for users with BIG-IP APM and IBM Security Access Manager

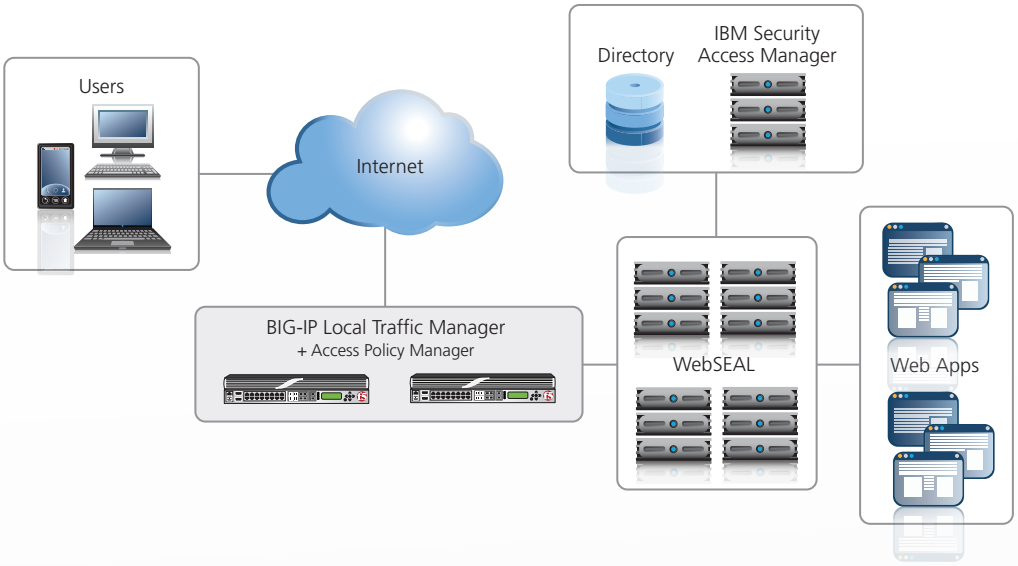
KEY BENEFITS

- High availability and scalability
- Secure web access
- Accelerated performance for remote and mobile users
- Single sign-on

THE CHALLENGES

The business perimeter has never been so permeable or difficult to defend. Employees, partners, and customers access critical applications and data from remote locations all over the world, using different networks and access devices and often without context or security. Whether applications reside in data centers, the cloud, or both, network administrators need more visibility and control over access by people who may be anywhere.

Yet sufficient monitoring and control systems can add complexity to the IT infrastructure and prove difficult and expensive to scale. The ability to deliver context-based access from a single policy control point is critical to managing a secure, scalable, and agile environment.



THE SOLUTION

Consolidate remote access, LAN access, and wireless connections within a single interface to streamline access management and ensure the security and availability of applications and data. F5® BIG-IP® Access Policy Manager® (APM) provides unified global access based on flexible access policies administered through a single, easy-to-use management interface.

Many web applications need to limit access by user. BIG-IP APM supports the necessary multi-factor authentication, authorization, and single sign-on (SSO) services. It works with IBM Security Access Manager to extend security policies across heterogeneous environments and into the cloud.

An integral part of the F5 application delivery firewall solution, BIG-IP APM complements IBM Security Access Manager in a unified and scalable solution that delivers secure access and protects assets from attack while ensuring efficient and integrated access management.

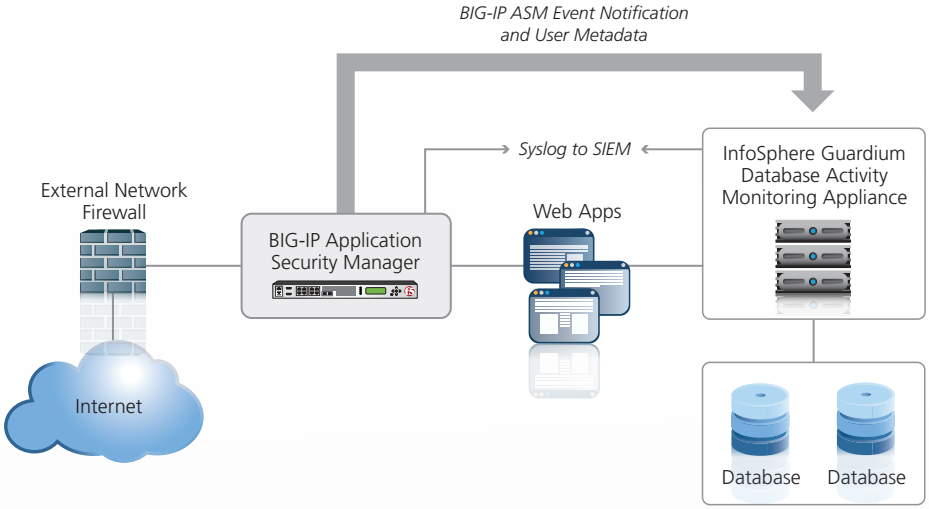
Defend your data, customers, and reputation with BIG-IP ASM and IBM InfoSphere Guardium

KEY BENEFITS

- Protection against unauthorized access
- Centralized end-to-end security monitoring and event correlation
- Streamlined security management

THE CHALLENGES

The proliferation of access devices and increasingly sophisticated attacks expose today's web applications to new vulnerabilities that can compromise your organization's data assets and reputation. A variety of technologies are available for protecting applications and databases from attack, but may lack the ability to work together to correlate a database attack with the source of the attack, including user metadata and other application layer information. To effectively protect data and thus the business, organizations need end-to-end web application and database security with unified notification, centralized policy management, and comprehensive reporting.



THE SOLUTION

By deploying F5 BIG-IP® Application Security Manager™ (ASM) with IBM InfoSphere Guardium Database Activity Monitoring, organizations can increase security visibility, receive immediate alerts about suspicious activity, and prevent attacks. Extensive, high-speed correlation of user identity data between BIG-IP ASM and InfoSphere Guardium ensures that web-based attempts to gain access to sensitive data, subvert the database, or execute denial-of-service (DoS) attacks can be recognized in context—and in real time—and stopped.

With this combined solution, malicious or compromised users can be isolated, forced to re-authenticate, or prevented from accessing applications. Threats are thus effectively blocked, now and in any subsequent attacks, with supporting correlation of data and consolidated reporting for follow-up, planning, and compliance auditing. By sharing user identity data in real time, BIG-IP ASM and InfoSphere Guardium proactively link a web application firewall with a data activity monitoring solution to achieve comprehensive security monitoring with a high level of correlation and insight.

Ensure application availability and integrity with BIG-IP ASM and IBM Security AppScan

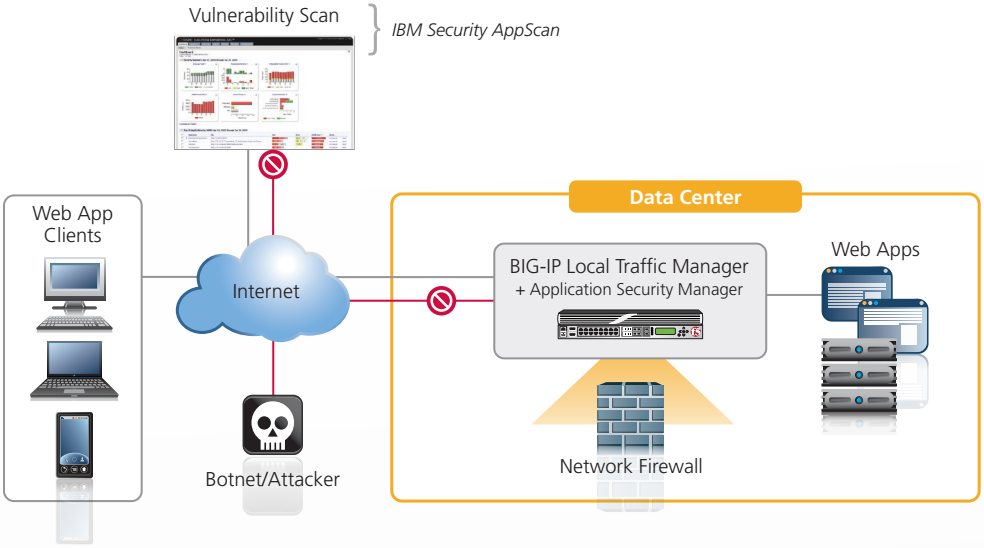
KEY BENEFITS

- Comprehensive protection from attacks
- Lower compliance costs
- Easier security policy management
- Flexible deployment in a virtual and private cloud environment

THE CHALLENGES

Web applications represent a critical, if not the primary, customer interface for a growing number of organizations. In this environment, network firewalls are no longer sufficient to protect applications. Today's multi-layer attacks increasingly target the application layer, where hidden vulnerabilities can be exploited with devastating effects on application availability, data security, customer confidence, and reputation, not to mention lost business and recovery costs.

Application scanners identify vulnerabilities, but correcting them takes time and resources while the vulnerabilities themselves remain open to exploit. Effective security requires the ability to not only identify weaknesses, but to immediately mitigate them to defeat emerging and opportunistic threats.



THE SOLUTION

BIG-IP Application Security Manager (ASM) secures applications in traditional, virtual, and private cloud environments, providing layer 7 protection against the latest threats, including distributed denial-of-service (DDoS) and diverse distributed denial-of-service (3DoS) attacks. IBM Security AppScan performs both source testing within the data center and dynamic testing at the Internet interface. BIG-IP ASM, in addition to being an effective web application firewall, works with IBM Security AppScan to secure applications against vulnerabilities.

BIG-IP ASM interfaces with IBM Security AppScan, processing scanning results so vulnerabilities can be rapidly mitigated with minimal effort through the BIG-IP ASM GUI. Vulnerability information can prompt quick, semi-automated creation and enforcement of new policies until recoding or other permanent fixes can occur. By combining data center and application firewall services with convenient management of scanning results and responses, BIG-IP ASM and IBM Security AppScan simplify the security infrastructure, increase the integrity of critical applications, and reduce the complexity and costs of security compliance.

Gain insight for managing infrastructure security with BIG-IP products and IBM Security QRadar

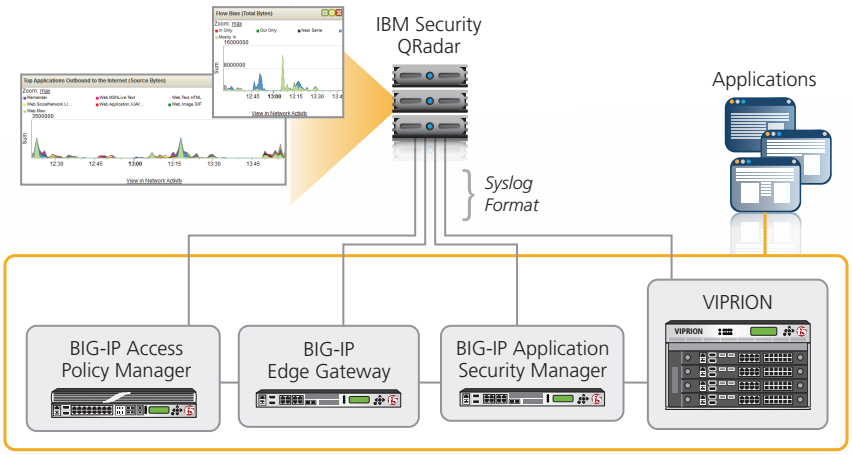
KEY BENEFITS

- Increased visibility into application traffic and events
- Lower security compliance and management costs
- Enhanced security posture analysis

THE CHALLENGES

Security analytics are becoming an increasingly vital weapon for maintaining information security despite sophisticated multi-level attacks, global botnets, and a rapidly evolving variety of access devices. Close monitoring of network access and use can enable quick detection of external threats or insider fraud and equip administrators to reduce business risk and ensure security compliance.

To be effective, however, security data from logging and monitoring must be timely and drawn from every part of the infrastructure in volumes that can become overwhelming. Meaningful analysis requires time-consuming data consolidation and correlation, particularly in complex infrastructures serving applications from multiple platforms and through the cloud.



THE SOLUTION

Gain crucial insight into security across the infrastructure with the network and event visibility provided by the BIG-IP product family, supplemented by the application monitoring capabilities of a security incident and event manager (SIEM) such as IBM's Security QRadar. F5 VIPRION® and the BIG-IP family of products, which reside at strategic points of control in the infrastructure, are uniquely positioned to monitor nearly all traffic in real time and consolidate key forensic data from across the infrastructure for SIEM analysis by IBM Security QRadar.

BIG-IP products deliver high-speed syslog and other logging data to IBM Security QRadar, which parses, correlates, and reports on infrastructure and application events and traffic. The F5 iControl® programming interface enables IT staff to easily control log management and interaction with IBM Security QRadar and streamline administration of the combined SIEM solution. Together, F5 products and IBM Security QRadar excel in both the comprehensive vision and execution considerations for SIEM, enabling sophisticated threat impact analysis, security measures that can be tailored to threats, and efficient management of the organization's comprehensive security posture.

LEARN MORE

To learn more about F5 and IBM security solutions, please visit **f5.com/ibm** and **f5.com/security**.

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

©2013 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS21-00005 0213