



F5 and Secerno

End-to-End Application and Database Security

About Secerno DataWall:

Secerno DataWall delivers advanced, comprehensive and intelligent database security. Organizations can choose to monitor database activity or deploy Secerno DataWall as a full database policy enforcement system.

The Secerno solution can be deployed in a rack-mounted appliance form factor or as a functionally equivalent virtual appliance deployed on a hardware platform of your choice, within a VMware® virtual environment.

Secerno's patented SynoptiQ™ Engine, uses Semantic Clustering™ to cluster queries automatically and intelligently into an Intent-Based Model™ of database environments. A zero-defect policy is automatically created, which identifies with fine precision and total accuracy every kind of query that is allowed – and specifies the actions to be taken on out-of-policy activity.

Uniquely, Secerno enforces a 100% positive security policy of only approved behavior, providing the option to either log, alert, block or substitute database requests. Policy Channels™ enable strategists and administrators to add new and complex layers of rules that map policy to a company's specific business needs.

Some of the most serious network security threats come from attacks that target vulnerabilities in enterprise applications. These attacks ignore conventional firewalls and intrusion-detection and prevention systems, and they are often difficult and costly to prevent.

BIG-IP Application Security Manager (ASM) delivers comprehensive protection for Web applications and operational infrastructure. BIG-IP ASM employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration makes implementation and maintenance easier, reducing the overall total cost of ownership.

Security professionals have long recognized the value of correlating security data coming from different vantage points. This can yield insights into security violations that would otherwise be difficult to detect. One such valuable combination involves correlating security data from both a web application firewall and a database firewall. Each firewall type offers a different vantage point on attacks, and when combined together they provide advanced protection that would otherwise be unavailable. In order to capitalize on this, F5 and Secerno have partnered to enable users of both products to correlate security information between F5's web application firewall appliance and Secerno's database firewall appliance: Secerno DataWall™. This provides enterprises with an end-to-end, layer 7 application and database security solution.

The Integrated Solution

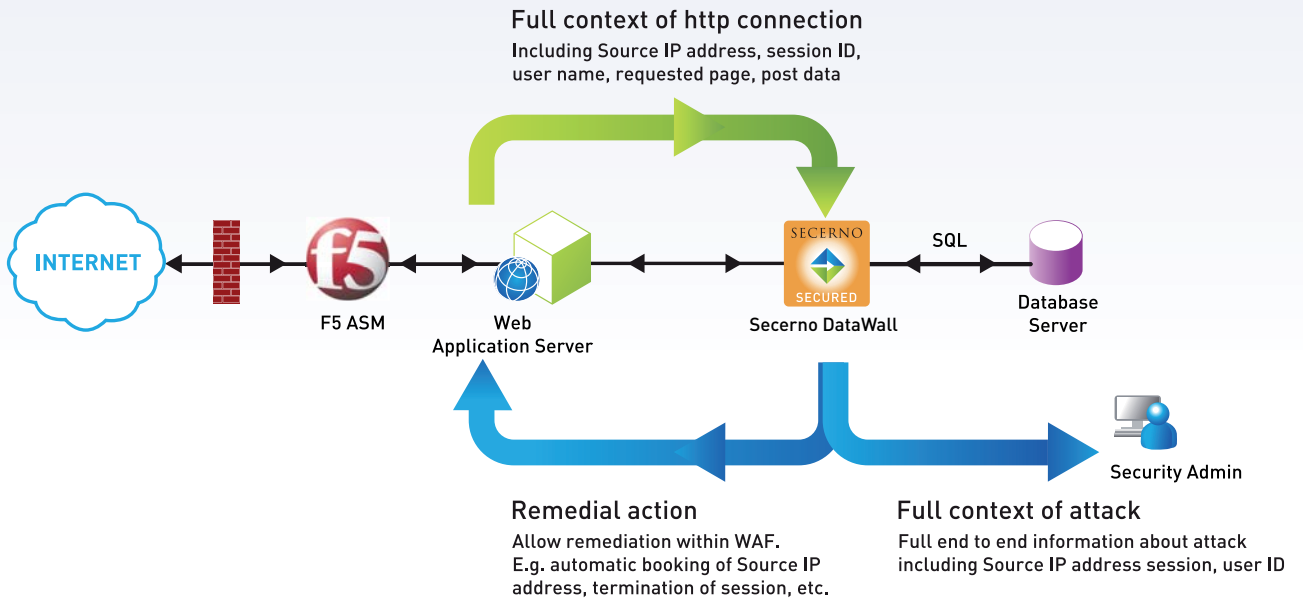
The integration between BIG-IP ASM and Secerno DataWall exposes the identity of users accessing the application so that deeper, more granular security policies can be used to secure an organization's valuable data.

The two solutions share common reporting for web-based attempts to gain access to sensitive data, subvert the database or execute Denial of Service (DoS) attacks against an organization's databases.

When threats to data are detected they are monitored, alerted or blocked and the identity of the user is shared between BIG-IP ASM and Secerno DataWall. To protect applications and databases, malicious or compromised users can be isolated, forced to re-authenticate or be prevented from accessing the application further, in real-time.

Furthermore, subsequent attacks from the same user can be prevented, diverted or rendered inert before the attacker can reach the application. Comprehensive alert and report information delivers immediate information on the type and severity of threats.

Sharing user identity between the F5 BIG-IP ASM and Secerno DataWall empowers those responsible for compliance auditing to unequivocally show, and report on over time, how an organization's data is being accessed – and by whom.



Summary

The combined solution of ASM and Secerno DataWall gives application business owners and security professionals alike the peace-of-mind that their application is benefiting from comprehensive threat prevention that includes protection of their core database assets, no matter from where they are accessed. They have an almost instantaneous remediation channel for either application code or database transactions which makes this a compelling solution for regulated environments with multiple technically diverse applications to protect.



**F5 Networks, Inc.
Corporate Headquarters**
401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com/info@f5.com

**F5 Networks
Asia-Pacific**
+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

**F5 Networks Ltd.
Europe/Middle-East/Africa**
+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeainfo@f5.com

**F5 Networks
Japan K.K.**
+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp