AppShield – Symantec Enterprise Security Architecture Solution Brief

Introduction

Never before has the need for application security been so obvious - or urgent. The Gartner Group estimates that 75% of all attacks are now occurring at the application level. At the recent Gartner Symposium/ITxpo 2003, Richard Clarke, the ex-White House cyber security czar outlined several trends that are quite telling. First, the number of security vulnerabilities has doubled every year for the last three years to as many as 60 new vulnerabilities per week. Second, the number of patches for those vulnerabilities has also doubled every year for the past three years, making patch management a road full of potholes. And finally, the time to exploit a vulnerability has gone from months to weeks to days, and now it's about six hours. Add to this an increasing rate of propagation of attacks, and it's no wonder the rising costs of cleanups are astounding. The worldwide cost in 2002 was $48 billion. The total projected worldwide cost for 2003 is between $119 billion to $145 billion.

There is no 'silver bullet' solution that solves all security threats today, thus customers typically deploy and manage a multi-layered, multi-vendor security solution. Fortunately, Sanctum and Symantec have teamed to solve many of the problems through an integrated, best-of-breed solution. Symantec's Enterprise Security Architecture (SESA) provides a standards-based interoperability framework for Symantec and Sanctum's solutions to work together and seamlessly deliver secure, manageable, and scalable enterprise security.

Sanctum's AppShield

AppShield™, an automated Web application firewall, provides maximum protection for Web applications fast. AppShield secures sites by blocking any type of application manipulation through the browser. AppShield 's *Positive Security* model identifies the legitimate requests made of an e-Business site and permits only those actions to take place. *No signature or patch management rule updates are required.* AppShield, therefore, ensures that the individual policies set for a site are complete and as up to date as the applications themselves. AppShield 4.0 secures your site by preventing, logging and alerting any type of application manipulation through the browser.

Symantec's Enterprise Security Architecture

Symantec™ Enterprise Security Architecture (SESA™) is a security software management infrastructure. It integrates multiple Symantec™ enterprise security and third-party products under a common user-interface framework to simplify monitoring and managing the multitude of security-related events that exist in today's corporate environments.

SESA's management product family, Symantec's Security Management System (SSMS), provides a 360° view into the security of the enterprise, a proactive stance to improve the overall security posture, and enables the customer to quickly and confidently take action in times of crisis. Using the Symantec Security Management System, enterprise customers will be

able to answer the questions: Am I at risk? Am I under attack? How should I respond to the attack? How effective is the response? Symantec's Security Management System allows for the consolidation of security events, the containment of security threats and the centralization of security policy enforcement.

Solution Overview

Customer environments are heterogeneous and often contain security products from many vendors. Therefore, an interoperable architecture is a critical enabler to enterprises that need strong security and centralized management. The Symantec Security Management System, as well as other Symantec products, are built in compliance with SESA which provides a standards-based interoperability framework for Symantec and third-party solutions to work together to provide secure, manageable, and scalable enterprise security

Sanctum has integrated AppShield with Symantec's Enterprise Security Architecture. Sanctum's AppShield will send relevant alarm and event information to SESA enabled products, adding crucial intelligence about threats at the application layer and enabling rapid response to complex security threats.

This best-of-breed combination from Symantec and Sanctum helps users identify and track the business impact of the most threatening application layer exploits, enabling customers to rapidly respond to complex security threats in order to reduce risk and control costs.

Key Benefits:

Reduce Business Risk:

- Enables comprehensive policy management and compliance from web application to the network down to the desktop. Symantec Enterprise Security Manager (ESM) 6.0 enables organizations to define, measure, and report on the compliance of information systems with pre-set corporate security policies, industry-standard security policies, or government regulations-all from a single console. Policy compliance data collected and analyzed by ESM can be correlated with security event data from a multitude of sources, including firewalls, intrusion detection systems, and vulnerability assessment products
- Improves ability to turn security data into prioritized, actionable information, enabling enterprises to respond rapidly to security breaches

Lower Cost of Operations:

- Reduces management complexity through consolidated logging, reporting, and ease-of-use
- Improves efficiency in responding to security threats by leveraging AppShield's crucial intelligence on application layer threats
- Facilitates security monitoring in the NOC (at a lower cost than a dedicated SOC) and extends security expertise and awareness deeper into the organization

Return on Investment:

- Extends value of SESA to include web application security, providing investment protection
- Extends the effectiveness of enterprise security policies and enforcing compliance

Solution Detail

Sanctum has developed a SESA collector to allow AppShield to communicate with SESA enabled management products. AppShield logs important detailed information about illegal behavior and attacks for the web applications it protects in its MySQL database. The Sanctum SESA collector is a software utility that runs on the AppShield server. This collector periodically queries the event log database and transforms the MySQL logs into SESA compliant logs. The newly formatted logs are then sent to the SESA agent, also residing on the AppShield server, which then forwards the information to the SESA management console. From there, either the Symantec Event Manager or Symantec Incident Manager (available in 2004) will process the information accordingly.

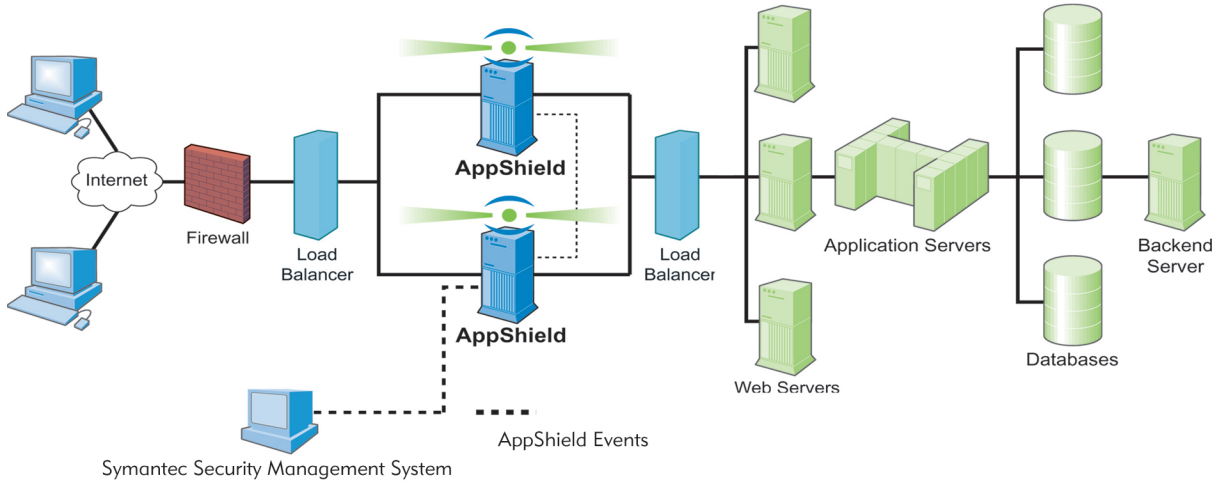

Figure 1: AppShield for Symantec Enterprise Security Architecture

More Information

http://www.sanctuminc.com/solutions/appshield/index.html

http://www.sanctuminc.com/partners/index.html