EMA Vendor to Watch: DB Networks

Value Proposition

It is estimated that SQL Injection (SQLi) is responsible for 90+% of the records losses on the Internet. OWASP and SANS publish SQLi as a top issue in every web application vulnerability report for the last 8 years. DB Networks was conceived to address this endemic problem. Current mainstream technologies such as Web Application Firewalls (WAF) and Intrusion Detection Sensors (IDS) are limited by their foundational architectures relying on either regular expressions (regex) to create signatures or behavioral analysis, which monitor for uncharacteristic actions between systems or protocols. These solutions experience multiple problems in detection. They are inherently fraught with high false alerting rates, warning that an attack is occurring during valid transactions (false positive) and producing no alerts when an actual attack is occurring (false negative). Estimates for out-of-the-box false alerting are 70+% for SQLi. (In comparison, DB Networks Core IDS's out-of-the-box false alert rate is less than 1%.) In most environments, these systems require significant man-hours of ongoing tuning, modifying signatures and behavior exceptions, to maintain moderate levels of accuracy. This is not true for DB Networks Core IDS technology. Though it uses the concept of behavioral analysis, it is not focused on the interactions of systems and protocols, it is focused on the SQL transaction itself. After installation, the Core IDS will alert the management station of all databases it identifies and any odd transactions, so any initial tuning can be done. It utilizes a committee of 14 unique judgment engines that each evaluate the structure of a database submission. Each engine presents its finding to the committee at a risk rating between 0 and 1; a 1 means it judges the risk of that transaction being malicious as 100%. Once the judges rule, based upon internal algorithms, transactions identified to be malicious are blocked and an alert is generated for the management console. All of the interaction details are maintained for future review, and visualization tools are built into the management console to show how an attack was introduced into the environment and how it progressed in its attempts to compromise the protected databases.

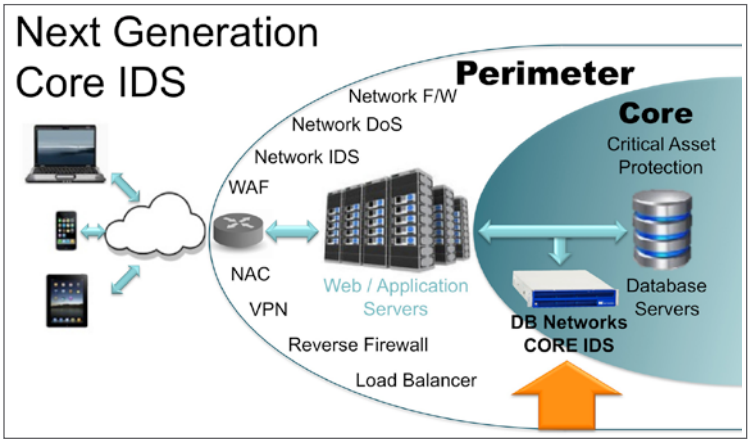

Figure 1: Inside the Core

EMA Perspective

The way the technology analyses transactions is fundamentally different from signature and traditional behavioral-based technology so Core IDS's capacity to identify an anomaly is much higher, with significantly greater accuracy against false alerts. While testing an out-of-the-box Core IDS instance with an up-to-date and somewhat customized Snort implementation in line Enterprise Management Associates (EMA) saw multiple SQLi variants pass undetected by Snort while Core IDS blocked them all. Comparing it to the leading WAF vendor, it required no evaluation of logs for regex or transaction tuning for false alerts.

The DB Networks solution is a highly focused product targeting a gap that is not being adequately addressed in many environments. For many enterprises, the web applications are high profile targets containing millions of confidential records. Considering, first, the cost and time for rewriting or upgrading/patching the myriad of applications; second, the time and money spent on purchasing and maintaining WAFs and IDSs; and third, the cost of breach at $130-$199 per record, it is easy to justify the expense for DB Networks Core IDS. The ROSI can be seen a few days after install. For the enterprise, it could save millions in lost revenue and brand degradation. For the SMB, it could mean the difference between being here today and gone tomorrow.

About Vendor to Watch

EMA Vendors to Watch are companies that deliver unique customer value by solving problems that had previously gone unaddressed or provide value in innovative ways. The designation rewards vendors that dare to go off the beaten path and have defined their own market niches.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook. 2733.102813