McAfee Enterprise Security Manager (ESM)

In the ever-changing marketplace of today's network security products, it is not uncommon to see a company acquire another company with the idea of taking a good product and making it better. We have seen firsthand that sometimes this works and sometimes it doesn't. However, in the case of McAfee, it has found a real winner with this product. The Enterprise Security Manager from McAfee is a new iteration of our old friend, the NitroView from NitroSecurity. When we see acquisitions such as these, it always makes us nervous because we fear that a good product can easily go bad. So far, this is not the case with this one. So what does the Enterprise Security Manager, or ESM, have to offer? A lot if you ask us. This product features a powerful correlation engine that is driven by an ultralight proprietary backend database. The ESM is able to gather, store and analyze logs and data from a large amount of sources and then correlate events based on rules, possible risk or historical trends.

SC MAGAZINE LAB APPROVED

An appliance that has this much power must be difficult to configure, right? Not at all. The initial setup process takes just a few minutes and can be done directly on the LCD screen on front of the appliance. This is where all the network configuration is done, and after the appliance is connected to the network all further management is done via a web GUI. We found this interface to be one of our favorite parts of the appliance. The management interface is loaded with visuals and dashboards that include many charts and graphs that can be drilled down into all the way to raw log data. Dashboards also can be customized to meet the analysis needs of the user by simply adding or removing the various dashboard modules.

This product can take logs from just about anything with an IP address, but what makes it stand out is its Database Activity Monitor and Application Data Monitor. Using these two features, security administrators can easily collect data from database and application logs for deep forensic analysis. The ESM also comes preloaded with more than 200 different predefined compliance report templates, along with a reporting function that enables the creation of custom reports quickly and easily.

Documentation included an installation and a full user guide. We found these materials to be complete and well-organized.

McAfee offers customers 24/7 phone- and email-based technical assistance as part of an annual agreement. Customers also can access a web-based portal via the website, which includes a knowledge base, downloads, support case management and other resources.

At a price just shy of $39,000, this product may seem quite expensive at first. However, we find that its combination of features, paired with the solid correlation engine and backend database, make it an excellent value for the money. The tool can provide security event management and analysis along with forensic capability that is easy to deploy for almost any size environment.

– Peter Stephenson, technology editor

DETAILS

Vendor	McAfee
Price	$38,995
Contact	mcafee.com
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Full SIEM appliance with a powerful correlation engine and ultralight database.

Weaknesses None that we found.

Verdict This old war horse just gets better and better with age and maturity. We are excited about the new home it has at McAfee. Once again this year, we designate it SC Lab Approved.