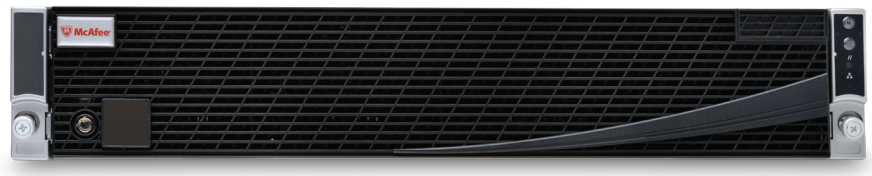

McAfee

Enterprise Security Manager

We have been watching this tool since it was born years ago as the NitroView SIEM. At that time, we said it was a vastly superior analysis tool but for user friendliness it had a way to go. A lot of its powerful functionality required a user with more than a little knowledge in the art of SIEM management. You certainly could not make that statement now. This is many times more powerful than those early models and so much is done automatically, if you wish, that it is a great SOC tool without sacrificing its value as an analyst tool.

This amazed us since the UI has not changed fundamentally since the first release. Moreover, it is a next-generation SIEM that is constantly evolving. Even so, it has immense functionality and integrates with a huge list of industry-standard log sources. The basic tool provides SIEM, compliance enterprise log management, network analysis functions and includes McAfee Event Receiver, which collects data for correlation and analysis by McAfee Enterprise Security Manager. It is licensed per VM instance.

Enterprise Security Manager – ESM – provides scalability and the performance needed for collecting and correlating massive volumes of log, flow and contextual data, including third-party threat feeds, application sessions and database activity. It provides simultaneous real-time and historical operations for optimizing threat investigations and forensics. While that is a bit of a mouthful, ESM does deliver. It comes standard with the McAfee Integrated Threat Defense and Global Threat Intelligence, but can consume threat feeds from a large number of third-party sources.

Other new features include access to a sandbox and preconfigured use cases. One of the challenges with earlier versions of ESM was setting up meaningful dashboards. That usually meant figuring out what you wanted to see in a particular use case, setting up a dashboard, a set of assets and weightings, and experimenting until you got just the right combination of displays to give a meaningful starting point for drilldown. True, there always have been some canned use cases supplied with the product but they were limited. Not anymore. Now the tool comes with dozens of preconfigured use cases and they are among the richest and most complete we've seen in any tool.

While the product is an on-premises tool, it communicates regularly with the McAfee cloud where it gets updates to such things as use cases, rules and content packs.

Documentation is excellent and support is comprehensive. Pricing is not inexpensive, but it is more than reasonable for this powerhouse. This is a tool that shines in a large environment, but we have used it in a much smaller venue with very good success. – *Peter Stephenson*

DETAILS

Vendor Intel Security

Price Starts at $39,995 for the VM software version or $47,994 for the hardware version.

Contact mcafee.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Probably the most comprehensive and powerful SIEM we've seen, continuing the legacy of the old Nitro product up to the present time.

Weaknesses None that we found.

Verdict For its performance, functionality and value, we are pleased to make Intel-McAfee one of our SC Lab Approved products and look forward to having in the SC Lab for a year's worth of evaluation.

Intel Security
2821 Mission College Boulevard
Santa Clara, CA 95054
888-847-8766 • www.mcafee.com/siem