Security Information & Event Management (SIEM)

McAfee Advanced Correlation Engine – identify and score threat events in real time using both rule- and risk-based logic.

McAfee

Features

Add-ons:

McAfee Advanced Correlation Engine – identify and score threat events in real time using both rule- and risk-based logic.

McAfee Application Data Monitor – monitor all the way to the application layer to detect fraud, data loss, and advanced threats. This SIEM tool supports accurate analysis of real application use, while enforcing policies and detecting malicious, covert traffic.

McAfee Database Event Monitor for SIEM – complete audit trail of all database activities, including queries, results, authentication activity, and privilege escalations, widening your visibility into who's accessing your data and why.

- McAfee Event Receiver – Collect up to tens of thousands of events per second with a single receiver.

McAfee Enterprise Log Manager – Reduce compliance costs with automated log collection, storage, and management. Collect, compress, sign, and store all original events with a clear audit trail of activity that can’t be repudiated.

McAfee Global Threat Intelligence for Enterprise Security Manager – Constantly updated threat intelligence feed that broadens situational awareness by enabling rapid discovery of events involving communications with suspicious or malicious IPs.

Description

A high-performance security information and event management (SIEM) solution brings event, threat, and risk data together to provide security intelligence, rapid incident response, seamless log management, and compliance reporting—delivering the context required for adaptive security risk management.

Specifications

Supported devices

System requirements

Processor

P4 class (not Celeron) or higher (Mobile/Xeon/Core2,Corei3/5/7)
AMD AM2 class or higher (Turion64/Athlon64/Opteron64,A4/6/8)
RAM — 1.5 GB

Windows operating system

- Windows 2000
- Windows XP
- Windows 2003 Server
- Windows Vista
- Windows 2008 Server
- Windows Server 2012
- Windows 7
- Windows 8
- Windows 8.1

Browsers

- Internet Explorer 9 or later
- Mozilla Firefox 9 or later
- Google Chrome 33 or later

Flash Player

- Version 11.2.x.x or later

Virtual Machine requirements

Processor — 8-core 64-bit, Dual Core2/Nehalem, or higher or AMD Dual Athlon64/Dual Opteron64 or higher

RAM — Depends on the model (4 GB or more)

Disk space — Depends on the model (250 GB or more)

ESM features use pop-up windows when uploading or downloading files. Disable the pop-up blocker for your ESM.

ESXi 5.0 or later

The minimum requirement is 250 GB unless the VM purchased has more. See the specifications for your VM product.

Links

Data Sheet
Solution Brief
Product Guide 9.6
Insurance Case Study

Sweden
Cognosec Nordic AB
Birger Jarlsgatan 12
114 34 Stockholm
Sweden
Tel +46 (0)8 400 170 00
sales.se@cognosec.com

UK & Ireland
Cognosec Limited
3rd Floor
The News Building
3 London Bridge Street
London SE1 9SG
UK
Tel +44 (0)20 3870 1539
sales.uk@cognosec.com

Germany
Cognosec GmbH
An der Welle 4
60322 Frankfurt
Germany
Tel +49 (0)69 7593 8490
sales.de@cognosec.com

Austria
Cognosec GmbH
Castellezgasse 16/2
1020 Vienna
Austria
Tel +43 (0)1 212 2020
sales.at@cognosec.com

UAE
Cognosec DMCC
2202 Indigo Icon Tower
Cluster F
Jumeirah Lakes Towers, Dubai
UAE
Tel +971 (0)4 451 1552
sales.dxb@cognosec.com