

Specification Sheet McAfee SIEM Appliances

| Product | Solution Description | Model Number | Maximum Ingestion EPS ¹ | Maximum Query EPS ² | Appliance Size | Local Storage ³ | Network Interfaces ⁴ | System Requirements |
|--|---|-------------------|------------------------------------|--------------------------------|----------------|-------------------------------|---------------------------------|------------------------------------|
| ESM-ELM-ERC "All-In-One" | Provides SIEM, Log Management, & Network Analysis functions. Includes McAfee Event Receiver. Provides Log Management and collects data for correlation and analysis by McAfee Enterprise Security Manager. | ESM-ELM-ERC-VM-8 | 1000 | 500 | VM | Recommended 250GB | VM (AWS, ESX, KVM) | 8 Processor Cores, 4GB of Memory |
| | | ESM-ELM-ERC-VM-12 | 5000 | 1500 | VM | Recommended 500GB + 480GB SSD | VM (AWS, ESX, KVM) | 12 Processor Cores, 64GB of Memory |
| | | ESM-ELM-ERC-5700 | 3500 | 1750 | 2U | 32 TB + 800GB SSD | 2 10Gb Ports | N/A |
| | | ESM-ELM-ERC-6050 | 7000 | 3500 | 2U | 40 TB + 800GB SSD | 2 10Gb Ports | N/A |
| Enterprise Security Manager (ESM) | McAfee Enterprise Security Manager provides Log Analysis, SIEM and Network Analysis functions. | ESM-VM-8 | 1500 | 500 | VM | Recommended 250GB | VM (AWS, ESX, KVM) | 8 Processor Cores, 4GB of Memory |
| | | ESM-VM-12 | 40,000 | 10,000 | VM | Recommended 500GB+480GB SSD | VM (AWS, ESX, KVM) | 12 Processor Cores, 64GB of Memory |
| | | ESM-VM-32 | 85,000 | 30,000 | VM | Recommended 2 TB+800GB SSD | VM (AWS, ESX, KVM) | 32 Processor Cores, 96GB of Memory |
| | | ESM-5700 | 65,000 | 20,000 | 2U | 32 TB + 800GB SSD | 2 10Gb Ports | N/A |
| | | ESM-6050 | 90,000 | 20,000 | 2U | 40 TB + 800GB SSD | 2 10Gb Ports | N/A |
| | | ESM-X7 | 200,000 | 35,000 | 2U | 16 TB SSD + 2 TB SSD (PCIe) | 2 10Gb Ports | N/A |
| | | ESM-X9 | 300,000 | 60,000 | 2U | 19 TB SSD + 8 TB SSD (PCIe) | 2 10Gb Ports | N/A |
| | | ESM-X11 | 400,000 | 80,000 | 2U | 19 TB SSD + 8 TB SSD (PCIe) | 2 10Gb Ports | N/A |
| Enterprise Log Manager (ELM) | McAfee Enterprise Log Manager provides Compliant Log Management functions. Requires an ESM and ERC. | ELM-VM-8 | 1500 | N/A | VM | Recommended 250GB | VM (AWS, ESX, KVM) | 8 Processor Cores, 4GB of Memory |
| | | ELM-VM-12 | 30,000 | N/A | VM | Recommended 500GB + 240GB SSD | VM (AWS, ESX, KVM) | 12 Processor Cores, 64GB of Memory |
| | | ELM-VM-32 | 70,000 | N/A | VM | Recommended 2 TB + 480GB SSD | VM (AWS, ESX, KVM) | 32 Processor Cores, 96GB of Memory |
| | | ELM-4700 | 55,000 | N/A | 2U | 5.6 TB SSD | 2 10Gb Ports | Requires an ESM and ERC |
| | | ELM-5700 | 75,000 | N/A | 2U | 32 TB + 800GB SSD | 2 10Gb Ports | Requires an ESM and ERC |
| | | ELM-6050 | 100,000 | N/A | 2U | 40 TB + 800GB SSD | 2 10Gb Ports | Requires an ESM and ERC |
| Direct Attached Storage (DAS) | For ESM and/or ELM, redundant architecture with RAID controller, mirrored cache, and IO multi-pathing. | DAS-50 | N/A | N/A | 4U | 50TB | N/A | Only for ESM, ELM |
| | | DAS-100 | N/A | N/A | 4U | 90TB | N/A | Only for ESM, ELM |
| Event Receiver (ERC) | McAfee Event Receiver collects 3rd party logs, events and flow data for correlation and analysis by McAfee Enterprise Security Manager. | ERC-VM-8 | 500 | N/A | VM | Recommended 250GB | VM (AWS, ESX, KVM) | 8 Processor Cores, 4GB of Memory |
| | | ERC-VM-12 | 5000 | N/A | VM | Recommended 500GB | VM (AWS, ESX, KVM) | 12 Processor Cores, 64GB of Memory |
| | | ERC-VM-32 | 15,000 | N/A | VM | Recommended 2 TB | VM (AWS, ESX, KVM) | 32 Processor Cores, 96GB of Memory |
| | | ERC-1270 | 7500 | N/A | 1U | 4 TB | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| | | ERC-2650 | 14,000 | N/A | 2U | 12 TB | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| | | ERC-3500 | 20,000 | N/A | 2U | 12 TB + 400GB SSD | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| | | ERC-4700 | 30,000 | N/A | 2U | 5.6 TB SSD | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| Advanced Correlation Engine (ACE) | Provides McAfee RSC and Enterprise correlation - identify and score threat events in real time or historical mode, using both rule- and risk-based logic, for McAfee Enterprise Security Manager. | ACE-VM-12 | <30000 | N/A | VM | Recommended 250GB | VM (AWS, ESX, KVM) | 12 Processor Cores, 64GB of Memory |
| | | ACE-VM-32 | <80,000 | N/A | VM | Recommended 500GB | VM (AWS, ESX, KVM) | 32 Processor Cores, 96GB of Memory |
| | | ACE-2650 | <75,000 | N/A | 2U | 12 TB | 2 10Gb Ports | Requires an ESM |
| | | ACE-4700 | <225,000 | N/A | 2U | 5.6 TB SSD | 2 10Gb Ports | Requires an ESM |
| Application Data Monitor (ADM) | McAfee Application Data Monitor decodes an application session to Layer 7, providing analysis of everything from the protocols and session integrity to the contents of the application itself (such as the text of an email or its attachments). | ADM-VM-8 | 250 Mbps | N/A | VM | Recommended 250GB | VM (ESX) | 8 Processor Cores, 4GB of Memory |
| | | ADM-VM-12 | 500 Mbps | N/A | VM | Recommended 500GB | VM (ESX) | 12 Processor Cores, 64GB of Memory |
| | | ADM-1270 | 1 Gbps | N/A | 1U | 4 TB | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| | | ADM-3500 | 1 Gbps | N/A | 2U | 12 TB | 2 10Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| Database Event Monitor (DEM) | McAfee Database Event Monitor offers detailed logging of databases & applications access. | DEM-2600 | 5000 | N/A | 2U | 1.8 TB | 2 1Gb Mgmt + 4 Monitor Ports | Requires an ESM |
| | | DEM-4600 | 15,000 | N/A | 2U | 3 TB | 2 1Gb Mgmt + 8 Monitor Ports | Requires an ESM |

Please refer to footnotes on bottom of page 2.

| Model Number | Dimensions | Input Voltage | Input Frequency | Power Supply | Power Consumption ⁵ | AMPS (Max) | MTBF/ Khrs | Weight lbs | Altitude (Max) | Temperature Operating | Altitude | BTU/Hr | Humidity |
|------------------|--------------------------------|----------------------------|-----------------|--------------|--------------------------------|------------------|------------|------------|--------------------------|---|---|----------------|--------------------------------------|
| ESM-X11 | 2U | 90V to 132V & 180V to 264V | 47 Hz to 63 Hz | 1100W x 2 | 904.7 | 4.1 | 38 | 49 lbs | Up to 10,000 ft | 10C to 35C (50F to 95F) | Up to 10,000 ft | 3085.1 | 50% to 90%, non-condensing |
| EXM-X9 | 3 1/2"H x 17 1/4" W x 28"L | | | | 850.4 | 3.9 | 38 | 49 | | | | 2899.7 | |
| ESM-X7 | | | | | 766 | 3.5 | 42 | 47 | | | | 2614.3 | |
| ESM-ELM-ERC-5700 | 2U | 90V to 132V & 180V to 264V | 47 Hz to 63 Hz | 1100W x 2 | 643.1 | 2.9 | 46 | 52 | Up to 10,000 (Operating) | 10C to 35C (50F to 95F) | Up to 10,000 (Operating) | 2192.9 | 50% to 90%, non-condensing |
| ESM-ELM-ERC-6050 | 3 1/2"H x 17 1/4" W x 28"L | | | | 754.5 | 3.4 | 42 | 56 | | | | 2572.8 | |
| ESM-5700 | | | | | 643.1 | 2.9 | 46 | 52 | | | | 2192.9 | |
| ESM-6050 | | | | | 754.5 | 3.4 | 42 | 56 | | | | 2572.8 | |
| ELM-4700 | | | | | 699.6 | 3.2 | 48 | 47 | | | | 2385.7 | |
| ELM-5700 | | | | | 643.1 | 2.9 | 46 | 52 | | | | 2192.9 | |
| ELM-6050 | | | | | 754.5 | 3.4 | 42 | 56 | | | | 2572.8 | |
| ERC-2650 | | | | | 572.1 | 2.6 | 53 | 46 | | | | 1950.7 | |
| ERC-3500 | | | | | 585.2 | 2.7 | 52 | 47 | | | | 1995.6 | |
| ERC-4700 | | | | | 699.6 | 3.2 | 48 | 47 | | | | 2385.7 | |
| ACE-2650 | | | | | 572.1 | 2.6 | 54 | 46 | | | | 1950.7 | |
| ACE-4700 | | | | | 699.6 | 3.2 | 48 | 47 | | | | 2385.7 | |
| ADM-3500 | | | | | 585.2 | 2.7 | 52 | 47 | | | | 1995.6 | |
| ERC-1270 | 1U | 90V to 132V & 180V to 264V | 47 Hz to 63 Hz | 350W x 1 | 192.6 | 1.8 | 194 | 20 | Up to 10,000 (Operating) | 10C to 35C (50F to 95F) | Up to 10,000 (Operating) | 656 | 50% to 90%, non-condensing |
| ADM-1270 | 1 5/8"H x 17 1/4" W x 21 5/8"L | | | | | | | | | | | | |
| DAS-50 | 4U | 110/220 VAC | 50/60 Hz | 1400W x 2 | 472W@110/220 VAC | 9.5@110/ 4.8@220 | N/A | 80 lbs | -45 to 9,500 Ft | 10° to 35° C (operating) -40° to 70° C (non-operating) | -45 to 9,500 Ft (operating) 45 to 25,000 Ft (non-operating) ¹ | BTU/HR 1609 | Operating 10% to 85%, non-condensing |
| DAS-100 | 7" H x 17.2"W x 27.5"L | | | | | | | 100 lbs | | | | | |

¹Maximum Ingestion Events Per Second (iEPS) describes peak advertised EPS for this appliance. iEPS is based on out-of-box settings with no adjustments to default event or flow aggregation and very limited overall SIEM user activity (Users, Alarms, Reports, IoCs, etc.). Any customization in the configuration or increase in user activity may result in reduced observed EPS rates.

²Maximum Query Events Per Second (qEPS) describes what a typical ESM appliance could expect to achieve under normal, active ESM usage conditions and reduced levels of event aggregation. Max qEPS assumes multiple analysts are accessing the system simultaneously while background activities such as Alarms, Reports and CyberThreat (IoC) queries are executing. In addition, Max qEPS assumes that customers would adjust the event and flow aggregation rates lower than out-of-box settings. McAfee recommends using qEPS numbers as the basis for sizing most ESM designs. Note that Max qEPS represents best performance estimates based on observations with typical larger enterprise customers; aggressive customizations or dramatic increases in user activity may result in reduced observed iEPS rates.

³This is the total raw, unformatted storage available for a given appliance. Please note that usable storage capacity may vary by as much as 40% less, depending on the model, based on RAID configuration, operating environment, data cardinality, software version, and a number of additional factors based on deployment customizations.

⁴For ERC, ADM and DEM models, the 2 MGMT ports are 10Gb and the 4 monitoring ports are 1Gb. For standalone ERC's, the 10Gb ports are used for management and event ingestion while the 1Gb monitoring ports are used for netflow monitoring via a SPAN port. For HA ERC's, the 10Gb ports are used for management and event ingestion while the 1Gb monitoring ports are used to connect the ERC HA pair together. For ADM and DEM, the 10Gb ports are used for management and the 1Gb monitoring ports are used to monitor application or database event traffic.

⁵Power consumption values may vary depending on the individual environment and system usage.

Please note that All McAfee SIEM appliances, except DAS-50 and DAS-100, have IPMI adapters. For ERC HA, the IPMI port is used for the HA configuration and cannot be used for remote management.

McAfee SIEM appliance specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, expressed or implied.