

McAfee Enterprise Security Manager (ESM) Supported Devices

McAfee® Enterprise Security Manager Data Sources Configuration Reference

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-----------------------------------|-------------------------------------|---|----------------------|------------|----------------------|-----------------|-----------|---------------------------------|
| A10 Networks | Load Balancer | Load Balancer | All | ASP | Syslog | 9.1 and above | AX Series | ✓ |
| Accellion | Secure File Transfer | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Access Layers | Portnox | NAC | 2.x | ASP | Syslog | 9.1 and above | | ✓ |
| Adtran | Bluesocket | Wireless Access Point | All | ASP | Syslog | 9.1.1 and above | | ✓ |
| AirTight Networks | SpectraGuard | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Alcatel-Lucent | NGN Switch | Switch | All | ASP | Syslog | 9.2 and above | | ✓ |
| | VitalQIP | Applications/Host/Server/ Operating Systems/Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| Amazon | CloudTrail | Generic | N/A | ASP | API | 9.5.1 and above | | ✓ |
| American Power Conversion | Uninterruptible Power Supply | Power Supplies | All | ASP | Syslog | 9.1 and above | | |
| Apache Software Foundation | Apache HTTP Server | Applications/Host/Server/ Operating Systems/Web Content/Filtering/Proxies | 1.x, 2.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | Apache Web Server | Applications/Host/Server/ Operating Systems/Web Content/Filtering/Proxies | 1.x, 2.x | ASP | Syslog | 9.1 and above | | |
| Apple Inc. | Mac OS X | Applications/Host/Server/ Operating Systems/Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| Arbor Networks | Peakflow SP | Network Switches and Routers | 2.x and above | ASP | Syslog | 9.2 and above | | |
| | Peakflow X | Network Switches and Routers | 2.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | Peakflow X | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | Pravail | IDS/IPS | All | ASP | Syslog | 9.1 and above | | ✓ |
| ArcSight | Common Event Format | Event Format | All | ASP | Syslog | 9.2 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------------|---|---|----------------------|------------|----------------------|-----------------|------------------|---------------------------------|
| Aruba | Aruba OS | Wireless Access Point | N/A | Code Based | Syslog | 9.1 and above | | |
| | ClearPass | Wireless Access Point | 5.x | ASP | Syslog | 9.1 and above | | ✓ |
| Attivo Networks | BOTSink | Generic | 3.3 and above | ASP | Syslog | 9.5.0 and above | | ✓ |
| Avecto | Privilege Guard (ePO) | IAM/IDM | 3.x | ASP | ePO - SQL | 9.2 and above | | |
| Axway | SecureTransport | Applications/Host/Server/ Operating Systems/Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| Barracuda Networks | Spam Firewall | Security Appliances/UTMs | 3.x, 4.x | ASP | Syslog | 9.1 and above | | ✓ |
| | Web Application Firewall | Security Appliances/UTMs | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Web Filter | Security Appliances/UTMs | All | ASP | Syslog | 9.1 and above | | ✓ |
| BeyondTrust | BeyondInsight | Auditing | 6.0 and above | ASP | Syslog | 9.6.0 and above | | |
| | BeyondTrust REM | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| | BeyondTrust Retina | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| Bit9 | Bit9 Security Platform/ Parity Suite - CEF | Application | All | ASP | Syslog | 9.2 and above | | ✓ |
| | Bit9 Security Platform/ Parity Suite | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Carbon Black | IDS/IPS | All | ASP | Syslog | 9.2 and above | | |
| Blue Coat | Director | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.2 and above | | ✓ |
| | ProxySG | Web Content/Filtering/Proxies | 4.x-6.x | ASP | Syslog | 9.1 and above | Access Log | ✓ |
| | Reporter | Application | 9.5.1 | ASP | Syslog | 9.5.0 and above | Cloud Access Log | ✓ |
| Blue Lance, Inc. | LT Auditor+ for Novell NetWare | Application | 9.x | Code Based | SQL | 9.1 to 9.3.2 | | |
| Blue Ridge Networks | BorderGuard | Firewall | 5000, 6000 | ASP | Syslog | 9.1 and above | | ✓ |
| BlueCat Networks | BlueCat DNS/DHCP Server | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Bradford Networks | Campus Manager | NAC/Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| Bro Network Security Monitor | Bro Network Security Monitor | Network Security | All | ASP | Syslog | 9.4 and above | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------|--------------------------------------|--|----------------------|------------|----------------------|---------------|--|---------------------------------|
| Brocade | BigIron, FastIron and NetIron | Network Switches and Routers | 7.5 and above | ASP | Syslog | 9.1 and above | | |
| | IronView Network Manager | NAC/Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | VDX Switch | Network Switches and Routers | All | ASP | Syslog | 9.2 and above | | ✓ |
| CA Technologies | DataMinder - CEF | DLP | All | ASP | Syslog | 9.1 and above | CEF Format | |
| | SiteMinder | Web Access | All | ASP | Syslog | 9.1 and above | | |
| Cerner | Cerner P2 Sentinel | Healthcare Auditing | All | Code Based | McAfee Event Format | 9.1 and above | | |
| Check Point | Check Point | Firewall | All | ASP | OPSEC | 9.3 and above | Firewall 1, Edge, Enterprise, Express, NG, NGX, SmartEvent and VPN | ✓ |
| | Check Point via Splunk | Firewall | All | ASP | Syslog | 9.2 and above | Using Splunk app | |
| Cimcor | CimTrak Management Console | Configuration Management | All | Code Based | McAfee Event Format | 9.1 and above | | |
| Cisco | ASA NSEL | Firewall/Flow | All | Netflow | Netflow | 9.1 and above | | |
| | CATOS v7xxx | Host/Server/Operating Systems/Network Switches and Routers | 6.x, 7.x | ASP | Syslog | 9.1 and above | | |
| | Content Services Switches | Other | All | ASP | Syslog | 9.1 and above | | |
| | CSA Console | Host/Server/Operating Systems/IDS/IPS | 5.x, 6.x | Code Based | SQL | 9.1 and above | | |
| | Guard DDoS Mitigator | IDS/IPS | All | ASP | Syslog | 9.1 and above | | |
| | Identity Services Engine | Other | All | ASP | Syslog | 9.1 and above | | |
| | IDS (4.x+ RDEP protocol) | IDS/IPS | 4.x and above | SDEE | | 9.1 and above | | |
| | IOS | IDS/IPS/Network Switches and Routers | 12.x and above | ASP | Syslog | 9.1 and above | ACL, IOS FW, IOS IDS and DSP | ✓ |
| | IOS ACL | Network Switches and Routers | 12.x and above | | | | Use Cisco IOS data source | ✓ |
| | IOS EAP | IDS/IPS/Network Switches and Routers | 12.x and above | | | | Use Cisco IOS data source | ✓ |
| | IOS Firewall | Firewall/Network Switches and Routers | 12.x and above | | | | Use Cisco IOS data source | ✓ |
| | IOS IDS | IDS/IPS/Network Switches and Routers | 12.x and above | | | | Use Cisco IOS data source | ✓ |
| | IOS IPS (SDEE protocol) | Application Protocol | All | SDEE | HTTP | 9.1 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-----------------------|--|--|----------------------|------------|----------------------|-----------------|---|---------------------------------|
| Cisco | IronPort Email Security | Email Security | 6.x, 7.x | ASP | Syslog | 9.1 and above | | |
| | IronPort Web Security Appliance | Web Content/Filtering/Proxies | 6.x, 7.x | ASP | Syslog | 9.1 and above | | |
| | Meraki | Wireless | All | ASP | Syslog | 9.4.1 and above | | ✓ |
| | MDS | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | NAC Appliance | NAC/Network Switches and Routers | All | ASP | Syslog | 9.1 and above | Formerly Clean Access | |
| | NAC Appliance (Clean Access) | NAC/Network Switches and Routers | 4.x | Code Based | HTTP | 9.1 to 9.3.2 | | |
| | NX-OS | IDS/IPS/Network Switches and Routers | 4.x, 5.x | ASP | Syslog | 9.1 and above | | ✓ |
| | Open TACACS+ | Authentication | All | ASP | Syslog | 9.1 and above | | |
| | PIX IDS | IDS/IPS/Network Switches and Routers | 12.x and above | | | | Use Cisco PIX/ASA/FWSM data source | ✓ |
| | PIX/ASA/FWSM | Firewall/IDS/IPS | 5.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| | Secure ACS | IDS/IPS | 3.x, 4.x | ASP | Syslog | 9.1 and above | | |
| | Unified Communications | Applications | All | ASP | Syslog | 9.2 and above | | |
| | Unified Computing System | Applications/Host/Server/Operating Systems/Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| | VSM/VPN Concentrator | Virtual Private Network | 2.x - 4.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | WAAS | Applications/Host/Server/Operating Systems/Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | |
| | WAP200 | Wireless Access Point | All | ASP | Syslog | 9.1 and above | | |
| | Wireless Control System | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | Wireless Lan Controller | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | NetScaler (AppFlow) | Flow | All | IPFix | IPFix | 9.2 and above | | |
| | Citrix | NetScaler (AppFlow) | Flow | All | IPFix | IPFix | 9.2 and above | |
| NetScaler | | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | Secure Gateway and NetScaler Web also supported | ✓ |
| Secure Gateway | | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.2 and above | | ✓ |
| Cluster Labs | Pacemaker | Application | 1.x | ASP | Syslog | 9.1 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-------------------------|---|------------------------------|---------------------------|------------|----------------------|-----------------|---|---------------------------------|
| Code Green | Data Loss Prevention | DLP | 8.x | ASP | Syslog | 9.1 and above | | ✓ |
| Cooper Power Systems | Cybectec RTU | Network Switches and Routers | 5.x, 6.x | ASP | Syslog | 9.1 and above | | ✓ |
| | Yukon IED Manager Suite | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Corero | Corero IPS | IDS/IPS | All | ASP | Syslog | 9.1 and above | | ✓ |
| Corvil | Security Analytics | Security Management | 9.1.1 and above | ASP | Syslog | 9.6 and above | | |
| Critical Watch | Critical Watch FusionVM | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| CyberArk | Enterprise Password Vault | Application | 5.x | ASP | Syslog | 9.1 and above | | ✓ |
| | Privileged Identity Management Suite -CEF | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Privileged Threat Analytics | UEBA | 3.1 | ASP | Syslog | 9.5.0 and above | CEF format is supported | ✓ |
| CyberGuard | CyberGuard | Firewall | 5.x | Code Based | Syslog | 9.1 to 9.3.2 | Includes FS, SG, SL | |
| Cyberoam | Cyberoam UTM and NGFW | UTM/Firewall | 10.0 and above | ASP | Syslog | 9.2 and above | | |
| Cylance | CylancePROTECT | Antivirus | 1.4.2 and above | ASP | Syslog | 9.6 and above | | |
| Cyrus | Cyrus IMAP and SASL | Messaging | 2.x | ASP | Syslog | 9.1 and above | | |
| D-Link | NetDefend UTM Firewall | UTM | All | ASP | Syslog | 9.2 and above | | |
| Damballa | Failsafe | Anti-Malware | All | ASP | Syslog | 9.1.1 and above | | ✓ |
| Dell | SonicWALL Aventail | Virtual Private Network | 10.x | ASP | Syslog | 9.1 and above | | ✓ |
| | SonicWALL SonicOS | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| | PowerConnect Switches | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| DenyAll | rWeb | Firewall/DoS | rweb 4.1, 4.1.1.1,4.1.3.2 | ASP | Syslog | 9.4.1 and above | | |
| DG Technology - InfoSec | Mainframe Event Acquisition System | MainFrame | 5.x, 6.x | ASP | Syslog | 9.1 and above | DG Technology MEASagent, DB2/IMS/Datacom/ID MS, CICS, FTP, MasterConsole, RACF/Top Secret/ACF2, Telnet, VSAM/BDAM/PDS, TCP/IP, SMP/E, | ✓ |
| Digital Defense | Digital Defense Frontline | Vulnerability Systems | All | N/A | N/A | 9.1.4 and above | | |
| Econet | Sentinel IPS | IDS/IPS | All | ASP | Syslog | 9.2 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|--------------------|---|-------------------------------|----------------------|------------|----------------------|-----------------|--|---------------------------------|
| EdgeWave | iPrism Web Security | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | |
| Enforcive | System z SMF DB2 | MainFrame | All | ASP | Syslog | 9.1 and above | Formerly Bsafe, AS/400, DB2/IMS/ Datacom/ID MS, FTP, RACF/Top Secret/ACF2, Telnet, VSAM/BDAM/PDS | |
| Enterasys Networks | Dragon IPS | IDS/IPS | 1.x-7.x | ASP | Syslog | 9.4 and above | | |
| | Dragon Sensor | IDS/IPS | 1.x-7.x | Code Based | SQL | 9.1 to 9.3.2 | | |
| | Dragon Squire | IDS/IPS | 1.x-7.x | Code Based | SQL | 9.1 to 9.3.2 | | |
| | Enterasys N and S Switches | Network Switches and Routers | 7.x | ASP | Syslog | 9.1 and above | | |
| | Enterasys Network Access Control | Network Switches and Routers | 7.x | ASP | Syslog | 9.1 and above | | |
| Entrust | IdentityGuard | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Epic | Clarity - CEF | Healthcare Application | 2015 and above | ASP | Syslog | 9.6 and above | Specific auditing events | ✓ |
| | Clarity - SQL Pull | Healthcare Application | 2010, 2012, 2014 | ASP | SQL | 9.4.0 and above | | ✓ |
| Exabeam | Exabeam UEBA | UEBA | 2.8 and above | ASP | Syslog | 9.6 and above | | |
| Extreme Networks | ExtremeWare XOS | Network Switches and Routers | 7.x, 8.x | ASP | Syslog | 9.1 and above | Alpine, BlackDiamond and Summit | ✓ |
| F5 Networks | BIG-IP Access Policy Manager | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | BIG-IP Application Security Manager - CEF | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.2 and above | | |
| | Firepass SSL VPN | Virtual Private Network | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Local Traffic Manager - LTM | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| FairWarning | Patient Privacy Monitoring | Application Security | 2.9.x | Code Based | McAfee EventFormat | 9.1 and above | | |
| Fidelis | Fidelis XPS | Network Security Appliance | All | ASP | Syslog | 9.1 and above | | ✓ |
| FireEye | FireEye Malware Protection System - CEF | Antivirus/Malware | 5.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| Fluke Networks | AirMagnet Enterprise | Network Switches and Routers | 8.x | ASP | Syslog | 9.1 and above | | ✓ |
| Force10 Networks | FTOS | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------------|-----------------------------------|------------------------------|----------------------|------------|----------------------|-----------------|----------|---------------------------------|
| ForeScout | CounterACT | Network Switches and Routers | 5.x and 6.x | ASP | Syslog | 9.1 and above | | ✓ |
| | CounterACT CEF | Network Switches and Routers | 7.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| Fortinet | FortiAuthenticator | Authentication | 3.x | ASP | Syslog | 9.2 and above | | |
| | FortiGate Antivirus | Antivirus | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | FortiGate Firewall | Firewall | 3.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | FortiGate IDS | IDS/IPS | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | FortiGate UTM - Comma Delimited | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| | FortiGate UTM - Space Delimited | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| | FortiMail | | | | | | | ✓ |
| | FortiManager | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| | FortiWeb Web Application Firewall | Firewall | All | ASP | Syslog | 9.1 and above | | |
| Fortscale | Fortscale UEBA | UEBA | 2.7 and above | ASP | Syslog | 9.5.0 and above | | ✓ |
| FreeRADIUS | FreeRADIUS | Authentication | All | ASP | Syslog | 9.1 and above | | ✓ |
| Fujitsu | IPCOM | Firewall/IDS/IPS | All | ASP | Syslog | 9.4 and above | | |
| Generic | Advanced Syslog Parser | Other | All | ASP | Syslog | 9.1 and above | | |
| | CIFS/SMB File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| | FTP/FTPS File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| | HTTP/HTTPS File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| | McAfee Event Format | Other | N/A | Code Based | McAfee EventFormat | 9.2 and above | | |
| | NFS File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| | SCP File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| | SFTP File Source | Other | N/A | Code Based | File pull | 9.2 and above | ELM only | |
| GFI | GFI LanGuard | VA Scanner | All | Code Based | File pull | 9.1 and above | | |
| Gigamon | GigaVUE | Switches and Routers | All | ASP | Syslog | 9.1.1 and above | | ✓ |
| Global Technology Associates | GNAT Box | Firewall | 5.3.x | ASP | Syslog | 9.1 and above | | |
| Globalscape | Globalscape EFT | File Transfer | 7.x | ASP | McAfee EventFormat | 9.4.1 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------------|--|-------------------------------------|-------------------------------|------------|----------------------|-----------------|---|---------------------------------|
| Good Technology | Good Mobile Control | Application | All | ASP | Syslog | 9.2 and above | | |
| Google | Search Appliance | Application | All | ASP | Syslog | 9.2 and above | | |
| HBGary | Active Defense | UTM | All | ASP | Syslog | 9.1 and above | | ✓ |
| Hewlett-Packard | 3Com Switches | Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | LaserJet Printers | Printers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | OpenVMS | Operating Systems | SYSLOG Client for OpenVMS 1.x | ASP | Syslog | 9.1 and above | Supported through "SYSLOG Client for OpenVMS", by Framework Solutions LLC | ✓ |
| | ProCurve | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Virtual Connect | Applicaton Devices | 4.4x | ASP | Syslog | 9.4.1 and above | | |
| Hitachi ID Systems | Identity and Access Management Suite | Authentication | | ASP | Syslog | 9.2 and above | | |
| HyTrust | HyTrust CloudControl | NAC | 3.x, 4.x | ASP | Syslog | 9.2 and above | | ✓ |
| IBM | DB2 LUW 9.5 and above, DB2 for Z/OS with CorreLog, DB2 for iSeries (AS/400) with Raz-Lee | Database | 8.x, 9.x, 10.x | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| | Guardium | Database Activity Monitoring | 6.x, 7.x | ASP | Syslog | 9.2 and above | | ✓ |
| | ISS Real Secure Server Sensor | Host/Server/OperatingSystems | 5.5 - 7.x | Code Based | SQL | 9.1 to 9.3.2 | | |
| | ISS SiteProtector | Security Management | All | Code Based | SQL | 9.1 and above | | |
| | MainFrame | MainFrame | All | | | | Use DG Technoloty MEAS Parser | |
| | Proventia GX | Other | All | ASP | Syslog | 9.1 and above | | |
| | System Z DB2 | Database | All | | | | Use DG Technoloty MEAS Parser | |
| | Tivoli Endpoint Manager - BigFix | Host/Server/OperatingSystems/ Other | All | ASP | Syslog | 9.1 and above | Linux Agent Required | |
| | Tivoli Identity Manager - SQL Pull | IAM/IDM | All | ASP | SQL | 9.2 and above | | |
| WebSphere Application Server | Application | 7.0 and above | ASP | File pull | 9.4.1 and above | | ✓ | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|---------------------|------------------------------------|--|----------------------|------------|----------------------|-----------------|-------------------------------|---------------------------------|
| IBM | WebSphere DataPower SOA Appliances | Application | 4.x | ASP | Syslog | 9.4.0 and above | | |
| | z/OS, z/VM | MainFrame | | | | | Use DG Technoloty MEAS Parser | |
| Imperva | WAF/DAM - CEF | Database | All | ASP | Syslog | 9.2 and above | | |
| Infoblox | NIOS | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| InfoExpress | CyberGatekeeper LAN | Network Switches and Routers | All | Code Based | Syslog | 9.1 to 9.3.1 | | |
| InterSect Alliance | Snare for AIX | Other | All | ASP | Syslog | 9.1 and above | | |
| | Snare for Solaris | Other | All | ASP | Syslog | 9.1 and above | | |
| | Snare for Windows | Other | All | ASP | Syslog | 9.1 and above | | ✓ |
| Intersect | Intersect | UEBA | 4.1 | ASP | Syslog | 9.5.1 and above | | ✓ |
| Invincea | Enterprise - CEF | Host/Server/OperatingSystems/ Other | All | ASP | Syslog | 9.1 and above | | |
| IPFIX | IPFIX | Network Flow Collection | All | IPFix | IPFix | 9.1 and above | | |
| Ipswitch | WS_FTP | Application | All | ASP | Syslog | 9.1 and above | | |
| iScan Online | iScan Online | Vulnerability Systems | All | N/A | N/A | 9.4 and above | | |
| Itron | Itron Enterprise Edition | Smart Grid Application | All | ASP | Syslog | 9.1 and above | | |
| Jflow | Jflow (Generic) | Network Flow Collection | 5, 7, 9 | Netflow | | 9.1 and above | | |
| Juniper Networks | Juniper Secure Access/MAG | VPN | All | ASP | Syslog | 9.1 and above | | |
| | JUNOS - Structured-Data Format | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| | JUNOS Router | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | NetScreen/IDP | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | NetScreen Firewall | Firewall | 4.x, 5.x, 6.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | NetScreen IDP | IDS/IPS | 3.x, 4.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | NetScreen SSL VPN Secure Access | VPN | 5.x - 7.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | Network and Security Manager - NSM | Applications/Host/Server / Operating Systems | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Secure Access version 7 | VPN | 5.x-7.x | ASP | Syslog | 9.1 and above | | |
| Steel Belted Radius | Radius Server | 5.x and above | ASP | Syslog | 9.1 and above | | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|--------------------|---|--------------------------------------|----------------------|------------|----------------------|-----------------|--|---------------------------------|
| Kaspersky | Administration Kit - SQL Pull | Antivirus | All | ASP | SQL | 9.2.1 and above | | ✓ |
| KEMP Technologies | LoadMaster | Network Switches and Routers | 4.x, 5.x | ASP | Syslog | 9.1 and above | | |
| Kerio Technologies | Kerio Control | Firewall | All | ASP | Syslog | 9.3.2 and above | | |
| Lancope | StealthWatch | IDS/IPS/Network Switches and Routers | 4.x-5.6 | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | StealthWatch | IDS/IPS/Network Switches and Routers | 6.x and above | ASP | Syslog | 9.1 and above | | |
| LANDESK | LANDESK | Vulnerability Systems | All | N/A | N/A | 9.4 and above | | |
| Legacy | Event Center | Other | All | ASP | Syslog | 9.1 and above | | |
| | Informant | IDS/IPS | All | ASP | Syslog | 9.3 and above | | |
| Lieberman | Enterprise Random Password Manager | Application | All | ASP | Syslog | 9.1.1 and above | XML | |
| Locum | RealTime Monitor | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| LOGbinder | LOGbinder for SharePoint (SP) | Application | 4.0, 5.0, 5.1 | ASP | Syslog | 9.2 and above | CEF and Standard Syslog formats are covered by the LOGbinder data source | ✓ |
| | LOGbinder for Exchange (EX) | Application | 2.0, 2.5, 3.0, 3.1 | ASP | Syslog | 9.2 and above | | ✓ |
| | LOGbinder for SQL Server (SQL) | Application | 1.5, 2.0, 2.1, 2.5 | ASP | Syslog | 9.2 and above | | ✓ |
| Lumension | Device Control - Endpoint Manager Security Suite (L.E.M.S.S.) | DLP | 8 | ASP | Syslog | 9.2.0 and above | | ✓ |
| | Bouncer - CEF | Application | 5.x and above | ASP | Syslog | 9.2 and above | | |
| | Bouncer | Application | 4.x | ASP | Syslog | 9.1 and above | | |
| | Lumension | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| Malwarebytes | Breach Remediation | Antivirus/Anti-Malware | 2.6.2 | ASP | Syslog | 9.5.0 and above | CEF syslog format is covered by the data source | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|---|--|--|----------------------|-------------|----------------------|-----------------|---|---------------------------------|
| Malwarebytes | Management Console | Antivirus/Anti-Malware | 1.7 | ASP | Syslog | 9.5.0 and above | Management Console, part of Malwarebytes Enterprise Endpoint Security, sends security events generated by Malwarebytes Anti-Malware and Malwarebytes Anti-Exploit running on managed endpoints. CEF formatted syslog is supported by ESM. | ✓ |
| MailGate, Ltd. | MailGate Server | Applications/Security Management/Host/Server / Operating Systems | 3.5 | ASP | Syslog | 9.1 and above | | |
| McAfee | Advanced Threat Defense | Anti-Malware | 3.2.2.4x and above | ASP | Syslog/DXL | 9.4.1 and above | | |
| | AntiSpyware (McAfee ePO Software) | Antivirus | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Application and Change Control (McAfee ePO Software) | Web Content/Filtering/Proxies | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Asset Manager Sensor | Asset Management | All | ASP | Syslog | 9.1.1 and above | | |
| | Correlation Engine | Other | All | Correlation | | 9.1 and above | | |
| | Database Security - CEF | Database | All | ASP | Syslog | 9.2 and above | | ✓ |
| | Database Security (McAfee ePO Software) | Database | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Deep Defender (McAfee ePO Software) | Other | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Email Gateway - CEF | Web Content/Filtering/Proxies | 6.x and above | ASP | Syslog | 9.2 and above | | ✓ |
| | EWS v5/Email Gateway OriginalFormat - Legacy | Web Content/Filtering/Proxies | 5.x | ASP | Syslog | 9.1 and above | | ✓ |
| | IronMail - Legacy | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | |
| | Endpoint Encryption (McAfee ePO Software) | Application | All | ASP | ePO - SQL | 9.3.2 and above | | ✓ |
| Endpoint Protection for Mac (McAfee ePO Software) | Antivirus | 2.0 and above | ASP | Syslog | 9.2.0 and above | | ✓ | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|---|--|---|----------------------|------------|----------------------|-----------------|-------|---------------------------------|
| McAfee | Endpoint Security Firewall (McAfee ePO Software) | Firewall | 10.2 and above | ASP | ePO - SQL | 9.5.0 and above | | ✓ |
| | Endpoint Security Platform (McAfee ePO Software) | Auditing | 10.2 and above | ASP | ePO - SQL | 9.5.0 and above | | ✓ |
| | Endpoint Security Threat Prevention (ePO) | Application | 10.2 and above | ASP | ePO - SQL | 9.5.0 and above | | ✓ |
| | Endpoint Security Web Control (McAfee ePO Software) | Application | 10.2 and above | ASP | ePO - SQL | 9.5.0 and above | | ✓ |
| | McAfee ePO Software Audit Log (McAfee ePO Software) | Other | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | ePolicy Orchestrator | Other | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | ePolicy Orchestrator Agent (McAfee ePO Software) | Applications/ SecurityManagement/Host/ Server/Operating Systems | 3.x and above | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Firewall Enterprise | Firewall/IDS/IPS | 8.x | ASP | Syslog | 9.2 and above | | ✓ |
| | Firewall for Linux (McAfee ePO Software) | Firewall | 8.x | ASP | Syslog | 9.5 and above | | ✓ |
| | Host Data Loss Prevention (McAfee ePO Software) | DLP | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Host Intrusion Prevention (McAfee ePO Software) | IDS/IPS | 6.x and above | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Informant | IDS/IPS | All | ASP | Syslog | 9.3 and above | | |
| | McAfee Advanced Correlation Engine | Correlation | All | | | 9.1 and above | | |
| | McAfee Application Data Monitor | Application | All | Code Based | | 9.1 and above | | |
| | McAfee Database Activity Monitor for SIEM | Database | All | Code Based | | 9.1 and above | | |
| | McAfee Enterprise Log Manager | | | | | | | |
| McAfee Enterprise Security Manager | | | | | | | | |
| McAfee Event Receiver | | | | | | | | |
| McAfee Event Receiver/ELM | | | | | | | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-------------------------------------|---|-------------------------------|----------------------|-----------|----------------------|--------------------------|---|---------------------------------|
| McAfee | McAfee Security for Domino Windows (McAfee ePO Software) | Web Content/Filtering/Proxies | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | McAfee Security for Microsoft Exchange (McAfee ePO Software) | Web Content/Filtering/Proxies | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | McAfee Vulnerability Manager | Vulnerability Systems | All | N/A | N/A | 9.1.2 and above | | ✓ |
| | MOVE AntiVirus (McAfee ePO Software) | Antivirus | All | ASP | ePO - SQL | 9.3.2 and above | | ✓ |
| | Network Access Control (ePO) | Other | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Network DLP Monitor | DLP | All | ASP | Syslog | 9.1 and above | | |
| | Network Security Manager - SQL Pull | IDS/IPS | 6.x and above | ASP | SQL | 9.1.2 and above | Formerly IntruShield | ✓ |
| | Network Security Manager | IDS/IPS | 6.x and above | ASP | Syslog | 9.1 and above | Formerly IntruShield | ✓ |
| | Network Threat Response | IDS/IPS | 4.0.0.5, 4.1 | ASP | Code Based API | 9.3-9.4, 9.4.1 and above | NTR 4.0.0.5 is supported on ESM 9.3.x - 9.4.0. NTR 4.1 is supported on ESM 9.4.1 and above. | ✓ |
| | Next Generation Firewall - Stonesoft | IDS/IPS | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Nitro IPS | IDS/IPS | All | ASP | Syslog | 9.1 and above | | |
| | One Time Password Server | Authentication | 3.1 | ASP | Syslog | 9.2 and above | | |
| | Policy Auditor (McAfee ePO Software) | Policy Server | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | SaaS Email Protection | Email Security | All | ASP | File Pull | 9.4.1 and above | Supports csv formatted reports | |
| | SaaS Web Protection | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | |
| | SiteAdvisor (McAfee ePO Software) | Other | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| Threat Intelligence Exchange | Reputation Server | 1.0.0 | ASP | ePO - DXL | 9.4.1 and above | | ✓ | |
| UTM Firewall | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|--------------------------------------|--|---|----------------------|------------|-------------------------------|-----------------|--|---------------------------------|
| McAfee | McAfee VirusScan® Software (McAfee ePO Software) | Antivirus | All | ASP | ePO - SQL | 9.2 and above | | ✓ |
| | Web Gateway | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| | WebShield | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| MEDITECH | Caretaker | HealthCare Application | All | ASP | Syslog | 9.1 and above | | |
| Microsoft | ACS - SQL Pull | Applications/Host/Server / Operating Systems | All | ASP | SQL | 9.1.3 and above | | ✓ |
| | Adiscon Windows Events | Applications/Host/Server / Operating Systems | All | Code Based | Syslog | 9.1 and above | | |
| | Assets via Active Directory | Asset | All | | | 9.1 and above | | ✓ |
| | Event Forwarding | Applications/Host/Server / Operating Systems | 2008 | WMI | MEF - McAfeeSIEM Agent | 9.1 and above | | |
| | Exchange | Applications/Host/Server/ Operating Systems | 2007, 2010, 2013 | ASP | File pull / McAfee SIEM Agent | 9.1 and above | Message Tracking Logs | ✓ |
| | Forefront Client Security | HIPS | 2010 | ASP | SQL | 9.1.1 and above | | ✓ |
| | Forefront EndPoint Protection | HIPS | 2010 | ASP | SQL | 9.1 and above | See System Center 2012 Endpoint Protection | ✓ |
| | Forefront Threat Management Gateway/ Internet Security and Acceleration - W3C | Firewall/Host/Server/Operating Systems/Web Content/ Filtering/Proxies /Virtual Private Networks | All | ASP | File pull | 9.1 and above | | ✓ |
| | Forefront Threat Management Gateway- SQL Pull | IDS/IPS | 2010 | ASP | SQL | 9.3 and above | | ✓ |
| | Forefront Unified Access Gateway | IDS/IPS | 2010 | ASP | Syslog | 9.1.1 and above | | ✓ |
| | Internet Authentication Service - Database Compatible Format | Web Content/Filtering/Proxies | 2008, 2008 R2,2012 | ASP | File Pull | 9.5.2 and above | Database- Compatible Format | ✓ |
| | Internet Authentication Service -Formatted | Web Content/Filtering/Proxies | 2000, 2003, 2008 | ASP | File Pull | 9.1 and above | IAS Legacy Format | ✓ |
| | Internet Authentication Service - XML | Web Content/Filtering/Proxies | 2008 R2, 2012 | ASP | File Pull | 9.1 and above | DTS Compliant Format | ✓ |
| Internet Information Services | Host/Server/OperatingSystems/ Web Content/Filtering/Proxies | All | Code Based | Syslog | 9.1 to 9.3.2 | | ✓ | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-------------|--|---|----------------------|------------------------------|------------------------------|---------------|---|---------------------------------|
| Microsoft | Internet Information Services - FTP | Host/Server/Operating Systems/Web Content / Filtering/Proxies | All | ASP | File pull/ McAfee SIEM Agent | 9.1 and above | | ✓ |
| | Internet Information Services - SMTP | Host/Server/Operating Systems/Web Content / Filtering/Proxies | All | ASP | File pull/ McAfee SIEM Agent | 9.2 and above | | ✓ |
| | Internet Information Services | Host/Server/Operating Systems/ Web Content/Filtering/Proxies | All | ASP | File pull/ McAfee SIEM Agent | 9.1 and above | | ✓ |
| | Microsoft Active Directory | Other | All | WMI | WMI | 9.1 and above | | ✓ |
| | Microsoft Exchange Server | Other | 2007, 2010 | WMI | WMI | 9.1 and above | | ✓ |
| | Microsoft SQL Server | Database | All | WMI | WMI | 9.1 and above | | ✓ |
| | MSSQL | Database | 2000 and above | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| | MSSQL Error Log | Database | All | ASP | File pull/ McAfee SIEM Agent | 9.2 and above | | |
| | MSSQL Server C2 Audit | Database | 2000, 2005, 2008 | Code Based | MEF - McAfee SIEM Agent | 9.1 and above | | |
| | Network Policy Server | Policy Server | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Operations Manager | Host/Server/Operating Systems | All | Code Based | SQL | 9.1 to 9.3.2 | | ✓ |
| | PhoneFactor | Application | All | ASP | Syslog | 9.1 and above | | |
| | SharePoint | Host/Server/File Management | 2007, 2010 | ASP | Syslog | 9.1 and above | | |
| | System Center 2012 EndPoint Protection | HIPS | 2012 | ASP | SQL | 9.1 and above | Supported through the Endpoint Protection -SQL Pull data source. | ✓ |
| | System Center Operations Manager | Security Management | 2007 | Code Based | MEF - McAfee SIEM Agent | 9.1 and above | | |
| | Windows DHCP | Debug DHCP Logs | 2003, 2008 | ASP | File pull/ McAfee SIEM Agent | 9.1 and above | | ✓ |
| Windows DNS | Debug DNS Logs | 2003, 2008 | ASP | File pull/ McAfee SIEM Agent | 9.1 and above | | ✓ | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|----------------------|-------------------------|--|--|------------|----------------------|-----------------|---|---------------------------------|
| Microsoft | Windows Event Log - CEF | Applications/Host/Server/Operating Systems | All | ASP | Syslog | 9.2 and above | | |
| | Windows Event Log - WMI | Applications/Host/Server/Operating Systems | XP, Windows 7, Windows 8, Windows 10, Server 2003, Server 2008, Server 2012, Server 2016 | WMI | WMI | 9.1 and above | Windows 8 is supported in ESM version 9.3.2 and above | ✓ |
| Mirage Networks | CounterPoint | NAC/Network Switches and Routers | 2.3.1 | Code Based | Syslog | 9.1 to 9.3.2 | | |
| Motorola | AirDefense | Wireless Switch | All | ASP | Syslog | 9.1 and above | | ✓ |
| | AirDefense Enterprise | Wireless Switch | All | Code Based | Syslog | 9.1 to 9.3.2 | | ✓ |
| NetApp | Data ONTAP | Storage | 7.x | ASP | Syslog | 9.1 and above | | |
| | DataFort | Storage Switch | All | ASP | Syslog | 9.1 and above | | |
| | FAS | Storage | All | | | 9.1 and above | Use NetApp DataOnTap data source | |
| NetFlow | Generic NetFlow | Flow | 5, 7, 9 | NetFlow | NetFlow | 9.1 and above | | |
| NetFort Technologies | LANGuardian | Applications/Security Management/Host/Server/Operating Systems | All | ASP | Syslog | 9.1 and above | | ✓ |
| NetIQ | Security Manager | Network Switches and Routers/ Security Management | 5.1 | ASP | Syslog | 9.1 and above | | |
| | Sentinel Log Manager | Network Switches and Routers/ Security Management | All | ASP | Syslog | 9.1 and above | | |
| NetWitness | Informer - CEF | Application | All | ASP | Syslog | 9.1 and above | | |
| | Spectrum - CEF | Malware | All | ASP | Syslog | 9.2 and above | URL Integration | ✓ |
| NGS | NGS SquirrelL | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| Niara | Niara | UEBA | 1.5 and above | ASP | Syslog | 9.5.0 and above | | ✓ |
| Niksun | NetDetector | Other | All | ASP | Syslog | 9.1 and above | | |
| Nokia | IPSO | Firewall | All | Code Based | Syslog | 9.1 to 9.3.2 | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------|---|---|---|------------|------------------------------|-----------------|--|---------------------------------|
| Nortel Networks | Contivity VPN | Network Switches and Routers | 7.x | Code Based | Syslog | 9.1 to 9.3.2 | | ✓ |
| | Contivity VPN | Network Switches and Routers | 7.x | ASP | Syslog | 9.4 and above | | ✓ |
| | Passport 8000 Series Switches | Network Switches and Routers | 7.x | ASP | Syslog | 9.1 and above | | ✓ |
| | VPN Gateway 3050 | Virtual Private Network | 8.x | ASP | Syslog | 9.1 and above | | |
| Novell | eDirectory | Applications/Security Management/Host/Server/ Operating Systems | All | ASP | Syslog | 9.2 and above | | ✓ |
| | Identity and Access Management - IAM | IAM/IDM | All | ASP | Syslog | 9.1 and above | | ✓ |
| nPulse | CPX Flow and Packet Capture | Packet Capture | All | N/A | N/A | 9.1 and above | URL Integration | |
| OpenVAS | OpenVAS | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| OpenVPN | OpenVPN | VPN | 2.1 and above | ASP | Syslog | 9.1 and above | | |
| Oracle | Directory Server Enterprise Edition | Authentication | 11 | ASP | Syslog | 9.4.0 and above | Also covers: Sun ONE Server and Sun Java Directory Server Enterprise Edition | |
| | Identity Manager - SQL Pull | IAM/IDM | 9.1.0.1 | ASP | SQL | 9.3.2 and above | | |
| | Internet Directory | Authentication | 11 | ASP | File pull/ McAfee SIEM Agent | 9.4.1 and above | | ✓ |
| | MySQL on Linux | Database | 5.1, 5.5, 5.6, and 5.7 on Linux | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| | Oracle | Database | 8.1.7 and above running on Sun Solaris, IBM AIX, Linux, HP-UX, Microsoft Windows, including Oracle RAC and Oracle Exadata | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| | Oracle Audit - SQL Pull | Database | 9i, 10g, 11g, 12c | ASP | SQL | 9.2.1 and above | Supports standard and fine grain audits as well as Unified Audits introduced in 12c. | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|--------------------|-------------------------------------|---------------------------------------|--------------------------------|--------|----------------------|-----------------|---|---------------------------------|
| Oracle | Oracle Audit - XML File Pull | Database | 10g, 11g, 12c | ASP | SQL | 9.4.0 and above | | ✓ |
| | Oracle Audit | Database | 9i, 10g, 11g, 12c | ASP | Syslog | 9.2.1 and above | | ✓ |
| | Audit Vault and Database Firewall | Database/Firewall | 12.x | ASP | Syslog | 9.3.0 and above | | |
| | Real Application Clusters - RAC | Database | 11g | ASP | File Pull | 9.4.0 and above | Parses the Event Manager Log (evmd.log) | |
| | Solaris Basic Security Module - BSM | Host/Server/OperatingSystems | 9.x, 10.x | ASP | Syslog | 9.1 and above | | |
| | WebLogic | Other | 8.1.x | ASP | Syslog | 9.1 and above | | |
| Osiris | Host Integrity Monitor | Host/Server/Operating Systems/IDS/IPS | | ASP | Syslog | 9.1 and above | ISAKMP, RADIUS, SECURITY, Accounting, RIP, VR messages only | |
| Palo Alto Networks | Palo Alto Firewalls | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| PhishMe | PhishMe Intelligence | Correlation | | ASP | Syslog | 9.5.0 and above | CEF format is supported | ✓ |
| | PhishMe Triage | Email Security | 2.0 and above | ASP | Syslog | 9.5.1 and above | CEF format is supported | ✓ |
| Postfix | Postfix | Application | All | ASP | Syslog | 9.1 and above | | |
| PostgreSQL | PostgreSQL | Database | 9.2 and above running on Linux | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| | PostgreSQL | Database | All | ASP | Syslog | 9.1 and above | | |
| PowerTech | Interact - CEF | Host | All | ASP | Syslog | 9.2 and above | | |
| Prevoty | Prevoty | Application Security | 3.2.1 | ASP | Syslog | 9.5.1 and above | Requires Log4j on Prevoty | |
| Proofpoint | Messaging Security Gateway | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Qualys | Qualys QualysGuard | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| Quest | ChangeAuditor for Active Directory | Applications | All | WMI | WMI | 9.1 and above | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-------------------|----------------------------------|--|--------------------------|---------------------|----------------------|-----------------|---|---------------------------------|
| Radware | AppDirector | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| | AppWall | Firewall | All | ASP | Syslog | 9.2 and above | | |
| | DefensePro | IDS/IPS | 2.4.3 and above | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | DefensePro | IDS/IPS | 2.4.3 and above | ASP | Syslog | 9.1 and above | | |
| | LinkProof/FireProof | Network Switches and Routers | All | ASP | Syslog | 9.1 and above | | |
| Rapid7 | Rapid7 Metasploit Pro | Vulnerability Systems | 3.x and above | N/A | N/A | 9.1 and above | | |
| | Rapid7 Nexpose | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| Raytheon | SureView | Application | All | ASP | Syslog | 9.1 and above | | ✓ |
| Raz-Lee Security | iSecurity Suite | Application | All | ASP | Syslog | 9.2 and above | | ✓ |
| Red Hat | JBoss/WildFly v8 | Application Server | Jboss 7.x WildFlyv8.x | ASP | Syslog | 9.4.1 and above | | ✓ |
| RedSeal Networks | RedSeal 6 | Risk Complianace | All | ASP | Syslog | 9.1 and above | | ✓ |
| Reversing Labs | N1000 Network Security Appliance | IDS/IPS | 3.2.1.2 | ASP | Syslog | 9.5.0 and above | | ✓ |
| RioRey | DDoS Protection | Firewall/DoS | RIOS 5.0, 5.1, 5.2 | ASP | Syslog | 9.2.0 and above | | ✓ |
| Riverbed | Steelhead | Security Appliances/UTMs | 5.x | ASP | Syslog | 9.1 and above | | ✓ |
| RSA | Authentication Manager | Authentication | 7.x | ASP | Syslog | 9.1 and above | | ✓ |
| SafeNet | Hardware Security Modules | Application Security | All | ASP | Syslog | 9.1 and above | | ✓ |
| Saint | Saint | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| SAP | SAP Version 5 | Applications/Security Management/Host/Server / Operating Systems | 5.x and 6.x | ABAP Module and ASP | Syslog | 9.1 and above | | ✓ |
| | Sybase | Database | 12.5 and above | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| Savant Protection | Savant - CEF | Anti-Malware | 3.x | ASP | Syslog | 9.2 and above | | |
| Secure Crossing | Zenwall | Applications/ SecurityManagement/Host/ Server/Operating Systems | All | ASP | Syslog | 9.1 and above | | |
| SecureAuth | IEP - Single Sign On | Authentication | 5.x | ASP | Syslog | 9.1 and above | | |
| Securonix | Risk and Threat Intelligence | UEBA | | Code Based | McAfee EventFormat | 9.1 and above | | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-----------------------------|---|-------------------------------|----------------------|------------|-----------------------------------|-----------------|---|---------------------------------|
| SendMail | Sentrion | Messaging | All | | | | Use Unix - Linux datasource | |
| Sentrigo | Hedgehog - CEF | Database | All | ASP | Syslog | 9.2 and above | | |
| sFlow | Generic sFlow | Network Flow Collection | All | sFlow | sFlow | 9.1 and above | | |
| Silver Spring Networks | Network Infrastructure | Smart Grid | All | ASP | File pull/ McAfee SIEMAgent | 9.1 and above | | |
| Skycure | Skycure Enterprise | Mobile Security | All | ASP | Syslog | 9.4.1 and above | | ✓ |
| Skyhigh Networks | Cloud Security Platform | DLP | 2.2 and above | ASP | Syslog | 9.5.1 and above | CEF format issupported | ✓ |
| SnapLogic | SnapLogic | Cloud Integration | All | ASP | Syslog | 9.2 and above | | |
| Software Product Research | DB2 Access Recording ServicesDBARS | Database | All | ASP | Syslog | 9.1 and above | | |
| SonicWALL | SonicWall Firewall/VPN | Firewall | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | SonicWall IPS | IDS/IPS | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| Sonus | GSX | VOIP | All | ASP | Syslog | 9.1 and above | | |
| Sophos | Email Security and Data Protection | Email Security | All | ASP | Syslog | 9.1 and above | | |
| | Sophos Antivirus | Antivirus | All | Code Based | SQL | 9.1 and above | | |
| | UTM and Next-Gen Firewall | UTM/Firewall | 9.1 | ASP | Syslog | 9.4.0 and above | | |
| | Web Security and Control | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| SourceFire | 3D Defense Center | IDS/IPS | 4.10 | | | | Use FireSIGHT Management Console -eStreamer | ✓ |
| | Snort NIDS | IDS/IPS | All | | | | Use SourceFireNS/RNA data source | |
| | FireSIGHT Management Console -eStreamer | IDS/IPS | 5.x, 6.x | Code Based | eStreamer | 9.1.1 and above | | ✓ |
| | SourceFire NS/RNA | IDS/IPS | All | ASP | Syslog | 9.1 and above | Includes Snort IDS | |
| Squid | Squid | Web Content/Filtering/Proxies | 1.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | Squid | Web Content/Filtering/Proxies | 2.5 | ASP | Syslog | 9.1 and above | | |
| SSH Communications Security | CryptoAuditor | Auditing | 1.5 | ASP | Syslog | 9.4.1 and above | | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|------------------------------|---|--|---|------------|----------------------|-----------------|---|---------------------------------|
| STEALTHbits | StealthINTERCEPT | HIDS | 3.1.262.1 | ASP | Syslog | 9.4 and above | CEF format issupported | ✓ |
| StillSecure | Strata Guard | Firewall/Security Management/IDS/IPS/Virtual PrivateNetworks | 5.x, 6.x | ASP | Syslog | 9.1 and above | | |
| Stonesoft Corporation | Next Generation Firewall | IDS/IPS | All | | | | Use McAfee Next Generation Firewall - Stonesoft | ✓ |
| Sun | iPlanet | Web Server | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| Symantec | Altiris Management Console | Asset | 7.x and above | | | 9.2 and above | | |
| | Antivirus Corporate Edition Server | Antivirus | 8.x, 9.x | Code Based | SQL | 9.1 and above | | |
| | Critical System Protection | IDS/IPS | 5.2 | Code Based | SQL | 9.1 to 9.3.2 | | |
| | Critical System Protection | IDS/IPS | 5.2 | ASP | SQL | 9.4 and above | | |
| | Endpoint Protection | Antivirus | 11.x | Code Based | Syslog | 9.1 to 9.3.2 | | ✓ |
| | Endpoint Protection | Antivirus | 11.x, 12.x | ASP | Syslog | 9.1 and above | | ✓ |
| | PGP Universal Server | Host/Server/OperatingSystems | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Symantec Data Loss Prevention | DLP | All | ASP | Syslog | 9.1 and above | | ✓ |
| | Symantec Messaging Gateway | Messaging | 2.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| | Symantec Web Gateway | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | ✓ |
| Synology | DiskStation Manager | Application | All | ASP | Syslog | 9.2 and above | | |
| Tenable | Tenable Nessus | Vulnerability Systems | 3.x, 4.x, 5.x, 6.x | N/A | N/A | 9.1 and above | | |
| Teradata | Teradata | Database | 12, 13, 13.10, 14,15, and 15.1 on Linux | | | 9.1 and above | Supported through McAfee Data Center Security Suite for Databases | |
| ThreatConnect | Threat Intelligence Platform | UEBA | 3.x and above | ASP | Syslog | 9.5.0 and above | | ✓ |
| Thycotic | Secret Server | Authentication | 8 | ASP | Syslog | 9.2 and above | | |
| TippingPoint | SMS | Security Management | 2.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| | TippingPoint | Security Management | 1.x, 2.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | UnityOne | IDS/IPS | All | ASP | Syslog | 9.1 and above | | |
| TITUS | Message Classification | Application | All | WMI | WMI | 9.2.1 and above | Supported through Microsoft Windows Event Log | ✓ |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|---------------------------------|-------------------------------------|---------------------------------|--|------------|----------------------|-----------------|---------------------------------|---------------------------------|
| Tofino Security | Tofino Firewall LSM | Firewall | All | ASP | Syslog | 9.1 and above | | ✓ |
| Topia Technology | Skoot | Application | All | ASP | Syslog | 9.2 and above | | ✓ |
| Townsend Security | AS/400 - CEF | Host/Server/OperatingSystems | All | ASP | Syslog | 9.2 and above | | |
| Trapezoid | Trust Control Suite | Application | All | ASP | Syslog | 9.2 and above | | |
| TrapX Security | DeceptionGrid | Generic | 5.x and above | ASP | Syslog | 9.5.0 and above | | ✓ |
| Trend Micro | Control Manager | Antivirus/Vulnerability Systems | 3.x, 5.x, 6.x | Code Based | SQL | 9.1 to 9.3.2 | | |
| | Control Manager - SQL Pull | Antivirus/Vulnerability Systems | 5.x | ASP | SQL | 9.1.3 and above | | |
| | Deep Discovery - CEF | Antivirus/Vulnerability Systems | All | ASP | Syslog | 9.2 and above | | |
| | Deep Security - CEF | HIDS | 6.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| | Deep Security Manager - CEF | HIDS | 6.x and above | ASP | Syslog | 9.1 and above | | ✓ |
| | InterScan Web Security Suite | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.1 and above | | |
| | OfficeScan | Antivirus/Vulnerability Systems | All | ASP | File pull | 9.2 and above | | ✓ |
| | OSSEC | FIM/HIDS | 1.x, 2.x | ASP | Syslog | 9.1 and above | | |
| Tripwire | Tripwire/nCircle IP360 | Vulnerability Systems | All | N/A | N/A | 9.1 and above | | |
| | Tripwire Enterprise | Database/SecurityManagement | 4.x | ASP | Syslog | 9.1 and above | | |
| | Tripwire For Server | Database/SecurityManagement | 4.x | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | Tripwire For Server | Database/SecurityManagement | 4.x | ASP | Syslog | 9.4 and above | | |
| Trustwave | Data Loss Prevention | DLP | 8.x | ASP | Syslog | 9.2 and above | | ✓ |
| | Network Access Control | NAC | 3.x | ASP | Syslog | 9.1 and above | | ✓ |
| | WebDefend | Web Content/Filtering/Proxies | 4.x | ASP | Syslog | 9.1 and above | | |
| Tufin | SecureTrack | Firewall/Auditing | All | ASP | Syslog | 9.2 and above | | |
| Type80 Security Software | SMA_RT | Host/Server/OperatingSystems | All | Code Based | Syslog | 9.1 to 9.3.2 | | |
| | SMA_RT | Host/Server/OperatingSystems | All | ASP | Syslog | 9.4 and above | | ✓ |
| UNIX | Linux | Host/Server/OperatingSystems | All | ASP | Syslog | 9.1 and above | | ✓ |
| | UNIX OS | Host/Server/Operating Systems | Solaris, Red Hat Linux, HP-UX, IBM AIX andSUSE | Code Based | Syslog | 9.1 to 9.3.2 | | ✓ |
| VanDyke Software | VShell | Application | 2.x, 3.x | ASP | Syslog | 9.1 and above | | |
| Vericept | Content 360 | DLP | 8.x | ASP | Syslog | 9.2 and above | Supported through Trustwave DLP | |

DATA SHEET

| Vendor | Name | Device Type | Version(s) Supported | Parser | Method of Collection | ESM Version | Notes | Data Source Configuration Guide |
|-------------------------|---------------------------------|-------------------------------|----------------------|--------|-------------------------------|-----------------|-------|---------------------------------|
| Verdasys | Digital Guardian | DLP | All | ASP | Syslog | 9.2 and above | | ✓ |
| VMware | AirWatch | Mobile Device Management | 7.3, 8.0 | ASP | Syslog | 9.4.1 and above | | |
| | vCenter Server | Application | All | ASP | Code Based API | 9.3.2 and above | | ✓ |
| | VMware | Application | 1.x-5.x | ASP | Syslog | 9.1 and above | | ✓ |
| Voltage Security | SecureData Enterprise | DLP | 5.7 | ASP | Syslog | 9.4.1 and above | | |
| Vormetric | Data Security | Application | 4.x | ASP | Syslog | 9.1 and above | | ✓ |
| WatchGuard Technologies | Firebox and X Series | Firewall | 8.x-11.x | ASP | Syslog | 9.1 and above | | ✓ |
| Wave Systems Corp | Safend Protector | DLP | All | ASP | Syslog | 9.2 and above | | |
| Websense | Cloud Web Security | HIDS | All | ASP | File pull / McAfee SIEM Agent | 9.3.2 and above | | |
| | Websense - CEF, Key Value Pair | Web Content/Filtering/Proxies | 7.7 and above | ASP | Syslog | 9.2 and above | | ✓ |
| | Websense Enterprise - SQL Pull | Web Content/Filtering/Proxies | 6.x, 7.x | ASP | SQL | 9.2.2 and above | | ✓ |
| Wurldtech | OpShield | Control Systems/Firewall | 1.7.1 | ASP | Syslog | 9.4.1 and above | | ✓ |
| Xirrus | 802.11abgn Wi-Fi Arrays | Switches and Routers | All | ASP | Syslog | 9.1 and above | | ✓ |
| Zenprise | Secure Mobile Gateway | Security Mobile Gateway | 5.x and above | ASP | Syslog | 9.1 and above | | |
| ZeroFOX | ZeroFOX | Application | All | ASP | Syslog | 9.2 and above | | ✓ |
| Zscaler | Nanolog Streaming Service (NSS) | Web Content/Filtering/Proxies | All | ASP | Syslog | 9.4.0 and above | | ✓ |



2821 Mission College Boulevard
 Santa Clara, CA 95054
 888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, and VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. All other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 3542_0917
 SEPTEMBER 2017