

McAfee SIEM Supported Devices

Updated September 2014

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
A10 Networks	Load Balancer (ASP)	Load Balancer	All	ASP	Syslog	9.1 and greater
Accellion	Secure File Transfer (ASP)	Application	All	ASP	Syslog	9.1 and greater
Access Layers	Portnox (ASP)	NAC	2.x	ASP	Syslog	9.1 and greater
Adtran	Bluesocket (ASP)	Wireless Access Point	All	ASP	Syslog	9.1.1 and greater
	NetVanta (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
Airtight Networks	SpectraGuard (ASP)	Application	All	ASP	Syslog	9.1 and greater
	NGN Switch (ASP)	Switch	All	ASP	Syslog	9.2 and greater
Alcatel-Lucent	VitalQIP (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
American Power Conversion	Uninterruptible Power Supply (ASP)	Power Supplies	All	ASP	Syslog	9.1 and greater
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 (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	1.x, 2.x	ASP	Syslog	9.1 and greater
Apple Inc.	Mac OS X (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
Arbor Networks	Peakflow SP (ASP)	Network Switches & Routers	2.x and greater	ASP	Syslog	9.2 and greater
	Peakflow X	Network Switches & Routers	2.x	Code Based	Syslog	9.1 to 9.3.2
	Peakflow X (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	Pravail (ASP)	IDS/IPS	All	ASP	Syslog	9.1 and greater
ArcSight	Common Event Format (ASP)	Event Format	All	ASP	Syslog	9.2 and greater
Aruba	Aruba OS	Wireless Access Point	N/A	Code Based	Syslog	9.1 and greater
	ClearPass (ASP)	Wireless Access Point	5.x	ASP	Syslog	9.1 and greater
Avecto	Privilege Guard (ePO)	IAM / IDM	3.x	ASP	ePO - SQL	9.2 and greater
Axway	SecureTransport (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
Barracuda Networks	Spam Firewall (ASP)	Security Appliances / UTMs	3.x, 4.x	ASP	Syslog	9.1 and greater
	Web Application Firewall (ASP)	Security Appliances / UTMs	All	ASP	Syslog	9.1 and greater
	Web Filter (ASP)	Security Appliances / UTMs	All	ASP	Syslog	9.1 and greater
BeyondTrust	BeyondTrust REM	Vulnerability Systems	All	N/A	N/A	9.1 and greater
	BeyondTrust Retina	Vulnerability Systems	All	N/A	N/A	9.1 and greater
Bit9	Bit9 Parity Suite - CEF (ASP)	Application	All	ASP	Syslog	9.2 and greater
	Bit9 Parity Suite (ASP)	Application	All	ASP	Syslog	9.1 and greater
Blue Coat	Director (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater
	ProxySG (ASP)	Web Content / Filtering / Proxies	4.x-6.x	ASP	Syslog	9.1 and greater
Blue Lance, Inc.	LT Auditor+ for Novell NetWare	Application	9.x	Code Based	SQL	9.1 to 9.3.2
Blue Ridge Networks	BorderGuard (ASP)	Firewall	5000, 6000	ASP	Syslog	9.1 and greater
BlueCat Networks	BlueCat DNS/DHCP Server (ASP)	Application	All	ASP	Syslog	9.1 and greater
Bradford Networks	Campus Manager (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater
Bro Network Security Monitor	Bro Network Security Monitor (ASP)	Network Security	All	ASP	Syslog	9.4 and greater
Brocade	BigIron, FastIron and NetIron (ASP)	Network Switches & Routers	7.5 and greater	ASP	Syslog	9.1 and greater
	IronView Network Manager (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	VDX Switch (ASP)	Network Switches & Routers	All	ASP	Syslog	9.2 and greater
CA Technologies	DataMinder - CEF (ASP)	DLP	All	ASP	Syslog	9.1 and greater
	SiteMinder (ASP)	Web Access	All	ASP	Syslog	9.1 and greater
Carbon Black	Carbon Black (ASP)	IDS / IPS	All	ASP	Syslog	9.2 and greater
Cerner	Cerner P2 Sentinel	Healthcare Auditing	All	Code Based	McAfee Event Format	9.1 and greater
Check Point	Check Point (ASP)	Firewall	All	ASP	OPSEC	9.3 and greater
	Check Point via Splunk (ASP)	Firewall	All	ASP	Syslog	9.2 and greater
Cimcor	CimTrak Management Console	Configuration Management	All	Code Based	McAfee Event Format	9.1 and greater
Cisco	ASA NSEL	Firewall / Flow	All	Netflow	Netflow	9.1 and greater
	CATOS v7xxx (ASP)	Host / Server / Operating Systems / Network Switches & Routers	6.x, 7.x	ASP	Syslog	9.1 and greater
	Content Services Switches (ASP)	Other	All	ASP	Syslog	9.1 and greater
	CSA Console	Host / Server / Operating Systems / IDS / IPS	5.x, 6.x	Code Based	SQL	9.1 and greater
	Guard DDoS Mitigator (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater
	Identity Services Engine (ASP)	Other	All	ASP	Syslog	9.1 and greater
	IDS (4.x+ RDEP protocol)	IDS / IPS	4.x and greater	SDEE		9.1 and greater
	IOS (ASP)	IDS / IPS / Network Switches & Routers	12.x and greater	ASP	Syslog	9.1 and greater
	IOS ACL	Network Switches & Routers	12.x and greater			
	IOS EAP	IDS / IPS / Network Switches & Routers	12.x and greater			
	IOS Firewall	Firewall / Network Switches & Routers	12.x and greater			
	IOS IDS	IDS / IPS / Network Switches & Routers	12.x and greater			
	IOS IPS (SDEE protocol)	Application Protocol	All	SDEE	HTTP	9.1 and greater
	IronPort Email Security (ASP)	Email Security	6.x, 7.x	ASP	Syslog	9.1 and greater
	IronPort Web Security Appliance (ASP)	Web Content / Filtering / Proxies	6.x, 7.x	ASP	Syslog	9.1 and greater
	MDS (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	NAC Appliance (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	NAC Appliance (Clean Access)	NAC / Network Switches & Routers	4.x	Code Based	HTTP	9.1 to 9.3.2
	NX-OS (ASP)	IDS / IPS / Network Switches & Routers	4.x, 5.x	ASP	Syslog	9.1 and greater
	Open TACACS+ (ASP)	Authentication	All	ASP	Syslog	9.1 and greater
	PIX IDS	IDS / IPS / Network Switches & Routers	12.x and greater			

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
	PIX/ASA/FWSM (ASP)	Firewall / IDS / IPS	5.x and greater	ASP	Syslog	9.1 and greater
	Secure ACS (ASP)	IDS / IPS	3.x, 4.x	ASP	Syslog	9.1 and greater
	Unified Communications (ASP)	Applications	All	ASP	Syslog	9.2 and greater
	Unified Computing System (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	VSM/VPN Concentrator	Virtual Private Network	2.x - 4.x	Code Based	Syslog	9.1 to 9.3.2
	WAAS (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	WAP200 (ASP)	Wireless Access Point	All	ASP	Syslog	9.1 and greater
	Wireless Control System (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	Wireless Lan Controller (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	NetScaler (AppFlow)	Flow	All	IPFix	IPFix	9.2 and greater
Citrix	NetScaler (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	Secure Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater
	Pacemaker (ASP)	Application	1.x	ASP	Syslog	9.1 and greater
Cluster Labs	Data Loss Prevention (ASP)	DLP	8.x	ASP	Syslog	9.1 and greater
Cooper Power Systems	Cybertec RTU (ASP)	Network Switches & Routers	5.x, 6.x	ASP	Syslog	9.1 and greater
	Yukon IED Manager Suite (ASP)	Application	All	ASP	Syslog	9.1 and greater
Corero	Corero IPS (ASP)	IDS/IPS	All	ASP	Syslog	9.1 and greater
Critical Watch	Critical Watch FusionVM	Vulnerability Systems	All	N/A	N/A	9.1 and greater
	Enterprise Password Vault (ASP)	Application	5.x	ASP	Syslog	9.1 and greater
CyberArk	Privileged Identity Management Suite - CEF (ASP)	Application	All	ASP	Syslog	9.1 and greater
	CyberGuard	Firewall	5.x	Code Based	Syslog	9.1 to 9.3.2
Cyberoam	Cyberoam UTM and NGFW	UTM / Firewall	10.0 and greater	ASP	Syslog	9.2 and greater
Cyrus	Cyrus IMAP & SASL (ASP)	Messaging	2.x	ASP	Syslog	9.1 and greater
D-Link	NetDefend UTM Firewall (ASP)	UTM	All	ASP	Syslog	9.2 and greater
Damballa	Failsafe (ASP)	Anti-Malware	All	ASP	Syslog	9.1.1 and greater
Dell	PowerConnect Switches (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
DG Technology - InfoSec	Mainframe Event Acquisition System (ASP)	MainFrame	5.x, 6.x	ASP	Syslog	9.1 and greater
Digital Defense	Digital Defense Frontline	Vulnerability Systems	All	N/A	N/A	9.1.4 and greater
Econet	Sentinel IPS (ASP)	IDS/IPS	All	ASP	Syslog	9.2 and greater
EdgeWave	iPrism Web Security (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
Enforcive	System z SMF DB2 (ASP)	MainFrame	All	ASP	Syslog	9.1 and greater
	Dragon IPS (ASP)	IDS/IPS	1.x-7.x	ASP	Syslog	9.4 and greater
Enterasys Networks	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 (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater
	Enterasys Network Access Control (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater
	IdentityGuard (ASP)	Application	All	ASP	Syslog	9.1 and greater
Epic	Clarity - SQL Pull (ASP)	Healthcare Application	2010, 2012, 2014	ASP	SQL	9.4.0 and greater
Extreme Networks	ExtremeWare XOS (ASP)	Network Switches & Routers	7.x, 8.x	ASP	Syslog	9.1 and greater
	BIG-IP Access Policy Manager (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
F5 Networks	BIG-IP Application Security Manager - CEF (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater
	Firepass SSL VPN (ASP)	Virtual Private Network	All	ASP	Syslog	9.1 and greater
	Local Traffic Manager - LTM (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
FairWarning	Patient Privacy Monitoring	Application Security	2.9.x	Code Based	McAfee Event Format	9.1 and greater
Fidelis	Fidelis XPS (ASP)	Network Security Appliance	All	ASP	Syslog	9.1 and greater
FireEye	FireEye Malware Protection System - CEF (ASP)	Antivirus/Malware	5.x and greater	ASP	Syslog	9.1 and greater
Fluke Networks	AirMagnet Enterprise (ASP)	Network Switches & Routers	8.x	ASP	Syslog	9.1 and greater
Force10 Networks	FTOS (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	CounterACT (ASP)	Network Switches & Routers	5.x and 6.x	ASP	Syslog	9.1 and greater
ForeScout	CounterACT CEF (ASP)	Network Switches & Routers	7.x and greater	ASP	Syslog	9.1 and greater
Fortinet	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 - (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
	FortiGate UTM - Space Delimited - (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
	FortiManager (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
	FortiWeb Web Application Firewall (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
FreeRADIUS	FreeRADIUS (ASP)	Authentication	All	ASP	Syslog	9.1 and greater
Generic	Advanced Syslog Parser	Other	All	ASP	Syslog	9.1 and greater
	CIFS/SMB File Source	Other	N/A	Code Based	File pull	9.2 and greater
	FTP/FTPS File Source	Other	N/A	Code Based	File pull	9.2 and greater
	HTTP/HTTPS File Source	Other	N/A	Code Based	File pull	9.2 and greater
	McAfee Event Format	Other	N/A	Code Based	McAfee Event Format	9.2 and greater
	NFS File Source	Other	N/A	Code Based	File pull	9.2 and greater
	SCP File Source	Other	N/A	Code Based	File pull	9.2 and greater
	SFTP File Source	Other	N/A	Code Based	File pull	9.2 and greater
GFI	GFI LanGuard	VA Scanner	All	Code Based	File pull	9.1 and greater
Gigamon	GigaVUE (ASP)	Switches & Routers	All	ASP	Syslog	9.1.1 and greater
Global Technology Associates	GNAT Box (ASP)	Firewall	5.3.x	ASP	Syslog	9.1 and greater
Good Technology	Good Mobile Control (ASP)	Application	All	ASP	Syslog	9.2 and greater
Google	Search Appliance (ASP)	Application	All	ASP	Syslog	9.2 and greater
HBGary	Active Defense (ASP)	UTM	All	ASP	Syslog	9.1 and greater
	3Com Switches (ASP)	Switches & Routers	All	ASP	Syslog	9.1 and greater
Hewlett-Packard	LaserJet Printers (ASP)	Printers	All	ASP	Syslog	9.1 and greater
	OpenVMS (ASP)	Operating Systems	1.x	ASP	Syslog	9.1 and greater
	ProCurve (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	Vertica	Database	5.1.1-0			9.1 and greater
HyTrust	HyTrust Appliance (ASP)	NAC	All	ASP	Syslog	9.2 and greater
	DB2	Database	8.x, 9.x, 10.x			9.1 and greater
IBM	Guardium (ASP)	Database Activity Monitoring	6.x, 7.x	ASP	Syslog	9.2 and greater
	Informix	Database	11.5			9.1 and greater
	ISS Real Secure Server Sensor	Host / Server / Operating Systems	5.5 - 7.x	Code Based	SQL	9.1 to 9.3.2
	ISS SiteProtector	Security Management	All	Code Based	SQL	9.1 and greater
	MainFrame	MainFrame	All			
	Proventia GX (ASP)	Other	All	ASP	Syslog	9.1 and greater
	System Z DB2	Database	All			

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
	Tivoli Endpoint Manager - BigFix (ASP)	Host / Server / Operating Systems / Other	All	ASP	Syslog	9.1 and greater
	Tivoli Identity Manager - SQL Pull (ASP)	IAM / IDM	All	ASP	SQL	9.2 and greater
	z/OS, z/VM	MainFrame				
Imperva	WAF/DAM - CEF (ASP)	Database	All	ASP	Syslog	9.2 and greater
Infoblox	NIOS (ASP)	Application	All	ASP	Syslog	9.1 and greater
InfoExpress	CyberGatekeeper LAN	Network Switches & Routers	All	Code Based	Syslog	9.1 to 9.3.1
InterSect Alliance	Soare for AIX (ASP)	Other	All	ASP	Syslog	9.1 and greater
	Soare for Solaris (ASP)	Other	All	ASP	Syslog	9.1 and greater
	Soare for Windows (ASP)	Other	All	ASP	Syslog	9.1 and greater
InterSystems	InterSystems Cache	Database	2011.1.x			9.1 and greater
Invincea	Enterprise - CEF (ASP)	Host / Server / Operating Systems / Other	All	ASP	Syslog	9.1 and greater
IPFIX	IPFIX	Network Flow Collection	All	IPFix	IPFix	9.1 and greater
Ipswitch	WS_FTP (ASP)	Application	All	ASP	Syslog	9.1 and greater
iScan Online	iScan Online	Vulnerability Systems	All	N/A	N/A	9.4 and greater
Itron	Itron Enterprise Edition (ASP)	Smart Grid Application	All	ASP	Syslog	9.1 and greater
Jflow	Jflow (Generic)	Network Flow Collection	5, 7, 9	Netflow		9.1 and greater
Juniper Networks	Juniper Secure Access/MAG (ASP)	VPN	All	ASP	Syslog	9.1 and greater
	JUNOS - Structured-Data Format (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	JUNOS Router (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	NetScreen / IDP (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	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 (ASP)	Applications / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater
	Secure Access version 7 (ASP)	VPN	5.x-7.x	ASP	Syslog	9.1 and greater
	Steel Belted Radius (ASP)	Radius Server	5.x and greater	ASP	Syslog	9.1 and greater
Kaspersky	Administration Kit - SQL Pull (ASP)	Antivirus	All	ASP	SQL	9.2.1 and greater
KEMP Technologies	LoadMaster (ASP)	Network Switches & Routers	4.x, 5.x	ASP	Syslog	9.1 and greater
Kerio Technologies	Kerio Control (ASP)	Firewall	All	ASP	Syslog	9.3.2 and greater
Lancope	StealthWatch	IDS / IPS / Network Switches & Routers	4.x-5.6	Code Based	Syslog	9.1 to 9.3.2
	StealthWatch (ASP)	IDS / IPS / Network Switches & Routers	6.x and greater	ASP	Syslog	9.1 and greater
LANDESK	LANDESK	Vulnerability Systems	All	N/A	N/A	9.4 and greater
Legacy	Event Center (ASP)	Other	All	ASP	Syslog	9.1 and greater
	Informant (ASP)	IDS / IPS	All	ASP	Syslog	9.3 and greater
Lieberman	Enterprise Random Password Manager (ASP)	Application	All	ASP	Syslog	9.1.1 and greater
Locum	RealTime Monitor (ASP)	Application	All	ASP	Syslog	9.1 and greater
LOGbinder	LOGbinder (ASP)	Application	All	ASP	Syslog	9.2 and greater
Lumension	Bouncer - CEF (ASP)	Application	5.x and greater	ASP	Syslog	9.2 and greater
	Bouncer (ASP)	Application	4.x	ASP	Syslog	9.1 and greater
	Lumension	Vulnerability Systems	All	N/A	N/A	9.1 and greater
MailGate, Ltd.	MailGate Server (ASP)	Applications / Security Management / Host / Server / Operating Systems	3.5	ASP	Syslog	9.1 and greater
McAfee	Advanced Threat Defense	Anti-Malware	3.2.2.4x and greater	ASP	Syslog / DXL	9.4.1 and greater
	AntiSpyware (ePO)	Antivirus	All	ASP	ePO - SQL	9.2 and greater
	Application and Change Control (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO - SQL	9.2 and greater
	Asset Manager Sensor (ASP)	Asset Management	All	ASP	Syslog	9.1.1 and greater
	Correlation Engine	Other	All	Correlation		9.1 and greater
	Database Security - CEF (ASP)	Database	All	ASP	Syslog	9.2 and greater
	Database Security (ePO)	Database	All	ASP	ePO - SQL	9.2 and greater
	Deep Defender (ePO)	Other	All	ASP	ePO - SQL	9.2 and greater
	Email Gateway - CEF (ASP)	Web Content / Filtering / Proxies	6.x and greater	ASP	Syslog	9.2 and greater
	EWS v5 / Email Gateway Original Format - Legacy - (ASP)	Web Content / Filtering / Proxies	5.x	ASP	Syslog	9.1 and greater
	IronMail - Legacy- (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	Endpoint Encryption (ePO)	Application	All	ASP	ePO - SQL	9.3.2 and greater
	Endpoint Protection for Mac (ASP)	Antivirus	2.0 and greater	ASP	Syslog	9.2.0 and greater
	ePO Audit Log (ePO)	Other	All	ASP	ePO - SQL	9.2 and greater
	ePolicy Orchestrator (ASP)	Other	All	ASP	ePO - SQL	9.2 and greater
	ePolicy Orchestrator Agent (ePO)	Applications / Security Management / Host / Server / Operating Systems	3.x and greater	ASP	ePO - SQL	9.2 and greater
	Firewall Enterprise (ASP)	Firewall / IDS / IPS	8.x	ASP	Syslog	9.2 and greater
	Host Data Loss Prevention (ePO)	DLP	All	ASP	ePO - SQL	9.2 and greater
	Host Intrusion Prevention (ePO)	IDS / IPS	6.x and greater	ASP	ePO - SQL	9.2 and greater
	Informant (ASP)	IDS / IPS	All	ASP	Syslog	9.3 and greater
	McAfee Advanced Correlation Engine	Correlation	All			9.1 and greater
	McAfee Application Data Monitor	Application	All	Code Based		9.1 and greater
	McAfee Database Event Monitor for SIEM	Database	All	Code Based		9.1 and greater
	McAfee Enterprise Log Manager					
	McAfee Enterprise Security Manager					
	McAfee Event Receiver					
	McAfee Event Receiver/ELM					
	McAfee Security for Domino Windows (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO - SQL	9.2 and greater
	McAfee Security for Microsoft Exchange (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO - SQL	9.2 and greater
	McAfee Vulnerability Manager	Vulnerability Systems	All	N/A	N/A	9.1.2 and greater
	MOVE AntiVirus (ePO)	Antivirus	All	ASP	ePO - SQL	9.3.2 and greater
	Network Access Control (ePO)	Other	All	ASP	ePO - SQL	9.2 and greater
	Network DLP Monitor (ASP)	DLP	All	ASP	Syslog	9.1 and greater
	Network Security Manager - SQL Pull (ASP)	IDS / IPS	6.x and greater	ASP	SQL	9.1.2 and greater
	Network Security Manager (ASP)	IDS / IPS	6.x and greater	ASP	Syslog	9.1 and greater
	Network Threat Response (ASP)	IDS / IPS	4.0.0.5, 4.1	ASP	Code Based API	9.3-9.4, 9.4.1 and greater
	Next Generation Firewall - Stonesoft (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater
	Nitro IPS	IDS / IPS	All	ASP	Syslog	9.1 and greater
	Policy Auditor (ePO)	Policy Server	All	ASP	ePO - SQL	9.2 and greater
	SaaS Web Protection (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	SiteAdvisor (ePO)	Other	All	ASP	ePO - SQL	9.2 and greater
	Threat Intelligence Exchange	Reputation Server	1.0.0	ASP	ePO - DXL	9.4.1 and greater

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
	UTM Firewall (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
	VirusScan (ePO)	Antivirus	All	ASP	ePO - SQL	9.2 and greater
	Web Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	WebShield (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
MEDITECH	Caretaker (ASP)	HealthCare Application	All	ASP	Syslog	9.1 and greater
Microsoft	ACS - SQL Pull (ASP)	Applications / Host / Server / Operating Systems	All	ASP	SQL	9.1.3 and greater
	Adiscon Windows Events	Applications / Host / Server / Operating Systems	All	Code Based	Syslog	9.1 and greater
	Assets via Active Directory	Asset	All			9.1 and greater
	Event Forwarding	Applications / Host / Server / Operating Systems	2008	WMI	MEF - McAfee SIEM Agent	9.1 and greater
	Exchange (ASP)	Applications / Host / Server / Operating Systems	2007, 2010	ASP	File pull / McAfee SIEM Agent	9.1 and greater
	Forefront Client Security (ASP)	HIPS	2010	ASP	SQL	9.1.1 and greater
	Forefront Endpoint Protection - SQL Pull (ASP)	HIPS	2010, 2012	ASP	SQL	9.1 and greater
	Forefront Threat Management Gateway / Internet Security and Acceleration - W3C (ASP)	Firewall / Host / Server / Operating Systems / Web Content / Filtering / Proxies / Virtual Private Networks	All	ASP	File pull	9.1 and greater
	Forefront Threat Management Gateway - SQL Pull (ASP)	IDS / IPS	2010	ASP	SQL	9.3 and greater
	Forefront Unified Access Gateway (ASP)	IDS / IPS	2010	ASP	Syslog	9.1.1 and greater
	Internet Authentication Service - Formatted (ASP)	Web Content/Filtering/Proxies	2003, 2008	ASP	Syslog	9.1 and greater
	Internet Authentication Service - XML (ASP)	Web Content/Filtering/Proxies	2003, 2008	ASP	Syslog	9.1 and greater
	Internet Information Services	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	Code Based	Syslog	9.1 to 9.3.2
	Internet Information Services - FTP (ASP)	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater
	Internet Information Services - SMTP (ASP)	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	File pull / McAfee SIEM Agent	9.2 and greater
	Internet Information Services (ASP)	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater
	Microsoft Active Directory	Other	All	WMI	WMI	9.1 and greater
	Microsoft Exchange Server	Other	2007, 2010	WMI	WMI	9.1 and greater
	Microsoft SQL Server	Database	All	WMI	WMI	9.1 and greater
	MSSQL	Database	7, 2000, 2005, 2008, 2012			9.1 and greater
	MSSQL Error Log (ASP)	Database	All	ASP	Syslog	9.2 and greater
	MSSQL Server C2 Audit	Database	2000, 2005, 2008	Code Based	MEF - McAfee SIEM Agent	9.1 and greater
	Network Policy Server (ASP)	Policy Server	All	ASP	Syslog	9.1 and greater
	Operations Manager	Host / Server / Operating Systems	All	Code Based	SQL	9.1 to 9.3.2
	PhoneFactor (ASP)	Application	All	ASP	Syslog	9.1 and greater
	SharePoint (ASP)	Host / Server / File Management	2007, 2010	ASP	Syslog	9.1 and greater
	System Center Operations Manager	Security Management	2007	Code Based	MEF - McAfee SIEM Agent	9.1 and greater
	Windows DHCP (ASP)	Debug DHCP Logs	2003, 2008	ASP	File pull / McAfee SIEM Agent	9.1 and greater
	Windows DNS (ASP)	Debug DNS Logs	2003, 2008	ASP	File pull / McAfee SIEM Agent	9.1 and greater
	Windows Event Log - CEF (ASP)	Applications / Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater
	Windows Event Log - WMI	Applications / Host / Server / Operating Systems	XP, Server 2003, Server 2008, Server 2012, Windows 7 and Windows 8	WMI	WMI	9.1 and greater
Mirage Networks	CounterPoint	NAC / Network Switches & Routers	2.3.1	Code Based	Syslog	9.1 to 9.3.2
Motorola	AirDefense (ASP)	Wireless Switch	All	ASP	Syslog	9.1 and greater
	AirDefense Enterprise	Wireless Switch	All	Code Based	Syslog	9.1 to 9.3.2
NetApp	Data ONTAP (ASP)	Storage	7.x	ASP	Syslog	9.1 and greater
	DataFort (ASP)	Storage Switch	All	ASP	Syslog	9.1 and greater
	FAS	Storage	All			9.1 and greater
NetFlow	Generic NetFlow	Flow	5, 7, 9	NetFlow	NetFlow	9.1 and greater
NetFort Technologies	LANGuardian (ASP)	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater
NetIQ	Security Manager (ASP)	Network Switches & Routers / Security Management	5.1	ASP	Syslog	9.1 and greater
	Sentinel Log Manager (ASP)	Network Switches & Routers / Security Management	All	ASP	Syslog	9.1 and greater
NetWitness	Informer - CEF (ASP)	Application	All	ASP	Syslog	9.1 and greater
	Spectrum - CEF (ASP)	Malware	All	ASP	Syslog	9.2 and greater
NGS	NGS SquirrelL	Vulnerability Systems	All	N/A	N/A	9.1 and greater
Niksun	NetDetector (ASP)	Other	All	ASP	Syslog	9.1 and greater
Nokia	IPSO	Firewall	All	Code Based	Syslog	9.1 to 9.3.2
Nortel Networks	Contivity VPN	Network Switches & Routers	7.x	Code Based	Syslog	9.1 to 9.3.2
	Contivity VPN (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.4 and greater
	Passport 8000 Series Switches (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater
	VPN Gateway 3050 (ASP)	Virtual Private Network	8.x	ASP	Syslog	9.1 and greater
Novell	eDirectory (ASP)	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater
	Identity and Access Management - IAM (ASP)	IAM / IDM	All	ASP	Syslog	9.1 and greater
nPulse	CPX Flow & Packet Capture	Packet Capture	All	N/A	N/A	9.1 and greater
OpenVAS	OpenVAS	Vulnerability Systems	All	N/A	N/A	9.1 and greater
OpenVPN	OpenVPN (ASP)	VPN	2.1 and greater	ASP	Syslog	9.1 and greater
Oracle	Identity Manager - SQL Pull (ASP)	IAM / IDM		ASP	SQL	9.3.2 and greater
	MySQL	Database	(32 bit, Windows) 4.x, 5.x, 6.x			9.1 and greater
	Oracle	Database	8.x, 9.x, 10g, 11g, 11g R2			9.1 and greater
	Oracle Audit - SQL Pull (ASP)	Database	10g, 11g	ASP	SQL	9.2.1 and greater
	Oracle Audit (ASP)	Database	All	ASP	Syslog	9.2.1 and greater

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
	Audit Vault and Database Firewall (ASP)	Database / Firewall	12.x	ASP	Syslog	9.3.0 and greater
	Solaris Basic Security Module - BSM (ASP)	Host / Server / Operating Systems	9.x, 10.x	ASP	Syslog	9.1 and greater
	WebLogic (ASP)	Other	8.1.x	ASP	Syslog	9.1 and greater
Osiris	Host Integrity Monitor (ASP)	Host / Server / Operating Systems / IDS / IPS		ASP	Syslog	9.1 and greater
Palo Alto Networks	Palo Alto Firewalls (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
Pivotal	Greenplum	Database	8.2.15			9.1 and greater
Postfix	Postfix (ASP)	Application	All	ASP	Syslog	9.1 and greater
PostgreSQL	PostgreSQL	Database	7.4.x, 8.4.x, 9.0.x, 9.1.x			9.1 and greater
	PostgreSQL (ASP)	Database	All	ASP	Syslog	9.1 and greater
PowerTech	Interact - CEF (ASP)	Host	All	ASP	Syslog	9.2 and greater
Proofpoint	Messaging Security Gateway (ASP)	Application	All	ASP	Syslog	9.1 and greater
Qualys	Qualys QualysGuard	Vulnerability Systems	All	N/A	N/A	9.1 and greater
Quest	ChangeAuditor for Active Directory	Applications	All	WMI	WMI	9.1 and greater
	AppDirector (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
	AppWall (ASP)	Firewall	All	ASP	Syslog	9.2 and greater
Radware	DefensePro	IDS / IPS	2.4.3 and greater	Code Based	Syslog	9.1 to 9.3.2
	DefensePro (ASP)	IDS / IPS	2.4.3 and greater	ASP	Syslog	9.1 and greater
	LinkProof/FireProof (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater
Rapid7	Rapid7 Metasploit Pro	Vulnerability Systems	3.x and greater	N/A	N/A	9.1 and greater
	Rapid7 Nexpose	Vulnerability Systems	All	N/A	N/A	9.1 and greater
Raytheon	SureView (ASP)	Application	All	ASP	Syslog	9.1 and greater
Raz-Lee Security	iSecurity Suite (ASP)	Application	All	ASP	Syslog	9.2 and greater
RedSeal Networks	RedSeal 6 (ASP)	Risk Compliance	All	ASP	Syslog	9.1 and greater
Riverbed	Steelhead (ASP)	Security Appliances / UTM's	5.x	ASP	Syslog	9.1 and greater
RSA	Authentication Manager (ASP)	Authentication	7.x	ASP	Syslog	9.1 and greater
SafeNet	Hardware Security Modules (ASP)	Application Security	All	ASP	Syslog	9.1 and greater
Saint	Saint	Vulnerability Systems	All	N/A	N/A	9.1 and greater
SAP	SAP Version 5 (ASP)	Applications / Security Management / Host / Server / Operating Systems	5.x and 6.x	ABAP Module & ASP	Syslog	9.1 and greater
	Sybase	Database	11.x, 12.x, 15.x			9.1 and greater
Savant Protection	Savant - CEF (ASP)	Anti-Malware	3.x	ASP	Syslog	9.2 and greater
Secure Crossing	Zenwall (ASP)	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater
SecureAuth	IEP - Single Sign On (ASP)	Authentication	5.x	ASP	Syslog	9.1 and greater
Securonix	Risk and Threat Intelligence	Application		Code Based	McAfee Event Format	9.1 and greater
SendMail	Sendmail	Messaging	All			
Sentriigo	Hedgehog - CEF (ASP)	Database	All	ASP	Syslog	9.2 and greater
sFlow	Generic sFlow	Network Flow Collection	All	sFlow	sFlow	9.1 and greater
Silver Spring Networks	Network Infrastructure (ASP)	Smart Grid	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater
SnapLogic	SnapLogic (ASP)	Cloud Integration	All	ASP	ASP	9.2 and greater
Software Product Research	DB2 Access Recording Services DBARS (ASP)	Database	All	ASP	Syslog	9.1 and greater
	Aventail (ASP)	Virtual Private Network	10.x	ASP	Syslog	9.1 and greater
	SonicOS (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
	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 (ASP)	VOIP	All	ASP	Syslog	9.1 and greater
	Email Security and Data Protection (ASP)	Email Security	All	ASP	Syslog	9.1 and greater
Sophos	Sophos Antivirus	Antivirus	All	Code Based	SQL	9.1 and greater
	Web Security and Control (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	3D Defense Center	IDS / IPS	4.10			
	Snort NIDS	IDS / IPS	All			
SourceFire	FireSIGHT Management Console - eStreamer	IDS / IPS	5.x.x	Code Based	eStreamer	9.1.1 and greater
	SourceFire NS/RNA (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater
Squid	Squid	Web Content / Filtering / Proxies	1.x	Code Based	Syslog	9.1 to 9.3.2
	Squid (ASP)	Web Content / Filtering / Proxies	2.5	ASP	Syslog	9.1 and greater
StillSecure	Strata Guard (ASP)	Firewall / Security Management / IDS / IPS / Virtual Private Networks	5.x, 6.x	ASP	Syslog	9.1 and greater
Stonesoft Corporation	Next Generation Firewall (ASP)	IDS / IPS	All			
Sun	iPlanet	Web Server	All	Code Based	Syslog	9.1 to 9.3.2
	Altiris Management Console	Asset	7.x and greater			9.2 and greater
	Antivirus Corporate Edition Server	Antivirus	8.x, 9.x	Code Based	SQL	9.1 and greater
	Critical System Protection	IDS / IPS	5.2	Code Based	SQL	9.1 to 9.3.2
	Critical System Protection (ASP)	IDS / IPS	5.2	ASP	SQL	9.4 and greater
	Endpoint Protection	Antivirus	11.x	Code Based	Syslog	9.1 to 9.3.2
	Endpoint Protection (ASP)	Antivirus	11.x, 12.x	ASP	Syslog	9.1 and greater
	PGP Universal Server (ASP)	Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater
	Symantec Data Loss Prevention (ASP)	DLP	All	ASP	Syslog	9.1 and greater
	Symantec Messaging Gateway (ASP)	Messaging	2.x and greater	ASP	Syslog	9.1 and greater
	Symantec Web Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
Synology	DiskStation Manager (ASP)	Application	All	ASP	Syslog	9.2 and greater
Tenable	Tenable Nessus	Vulnerability Systems	3.x, 4.x, 5.x, 6.x	N/A	N/A	9.1 and greater
Teradata	Teradata	Database	12.x, 13.x, 14.x			9.1 and greater
	SMS (ASP)	Security Management	2.x and greater	ASP	Syslog	9.1 and greater
TippingPoint	TippingPoint	Security Management	1.x, 2.x	Code Based	Syslog	9.1 to 9.3.2
	UnityOne (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater
TITUS	Message Classification	Application	All	WMI	WMI	9.2.1 and greater
Tofino Security	Tofino Firewall LSM (ASP)	Firewall	All	ASP	Syslog	9.1 and greater
Topia Technology	Skoot (ASP)	Application	All	ASP	Syslog	9.2 and greater
Townsend Security	AS/400 - CEF (ASP)	Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater
Trapezoid	Trust Control Suite (ASP)	Application	All	ASP	Syslog	9.2 and greater
	Control Manager	Antivirus / Vulnerability Systems	3.x, 5.x, 6.x	Code Based	SQL	9.1 to 9.3.2
	Control Manager - SQL Pull (ASP)	Antivirus / Vulnerability Systems	5.x	ASP	SQL	9.1.3 and greater
	Deep Discovery - CEF (ASP)	Antivirus / Vulnerability Systems	All	ASP	Syslog	9.2 and greater
	Deep Security - CEF (ASP)	HIDS	6.x and greater	ASP	Syslog	9.1 and greater
	Deep Security Manager - CEF (ASP)	HIDS	6.x and greater	ASP	Syslog	9.1 and greater
	InterScan Web Security Suite (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater
	OfficeScan (ASP)	Antivirus / Vulnerability Systems	All	ASP	Syslog	9.2 and greater
	OSSEC (ASP)	FIM / HIDS	1.x, 2.x	ASP	Syslog	9.1 and greater
	Tripwire / nCircle IP360	Vulnerability Systems	All	N/A	N/A	9.1 and greater

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version
Tripwire	Tripwire Enterprise (ASP)	Database / Security Management	4.x	ASP	Syslog	9.1 and greater
	Tripwire For Server	Database / Security Management	4.x	Code Based	Syslog	9.1 to 9.3.2
	Tripwire For Server (ASP)	Database / Security Management	4.x	ASP	Syslog	9.4 and greater
Trustwave	Network Access Control (ASP)	NAC	3.x	ASP	Syslog	9.1 and greater
	Vericept - CEF (ASP)	DLP	8.x	ASP	Syslog	9.2 and greater
	WebDefend (ASP)	Web Content / Filtering / Proxies	4.x	ASP	Syslog	9.1 and greater
Tufin	SecureTrack (ASP)	Firewall / Auditing	All	ASP	Syslog	9.2 and greater
Type80 Security Software	SMA_RT	Host / Server / Operating Systems	All	Code Based	Syslog	9.1 to 9.3.2
	SMA_RT (ASP)	Host / Server / Operating Systems	All	ASP	Syslog	9.4 and greater
	Linux (ASP)	Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater
UNIX	UNIX OS	Host / Server / Operating Systems	Solaris, Red Hat Linux, HP-UX, IBM AIX and SUSE	Code Based	Syslog	9.1 to 9.3.2
VanDyke Software	VShell (ASP)	Application	2.x, 3.x	ASP	Syslog	9.1 and greater
Verdasys	Digital Guardian (ASP)	DLP	All	ASP	Syslog	9.2 and greater
VMware	vCenter Server (ASP)	Application	All	ASP	Code Based API	9.3.2 and greater
	VMware (ASP)	Application	1.x-5.x	ASP	Syslog	9.1 and greater
Vormetric	Data Security (ASP)	Application	4.x	ASP	Syslog	9.1 and greater
WatchGuard Technologies	Firebox and X Series (ASP)	Firewall	8.x-11.x	ASP	Syslog	9.1 and greater
Wave Systems Corp	Safend Protector (ASP)	DLP	All	ASP	Syslog	9.2 and greater
Websense	Websense - CEF, Key Value Pair (ASP)	Web Content / Filtering / Proxies	7.7 and greater	ASP	Syslog	9.2 and greater
	Websense Enterprise - SQL Pull (ASP)	Web Content / Filtering / Proxies	6.x, 7.x	ASP	SQL	9.2.2 and greater
Xirrus	802.11abgn Wi-Fi Arrays (ASP)	Switches & Routers	All	ASP	Syslog	9.1 and greater
Zenprise	Secure Mobile Gateway (ASP)	Security Mobile Gateway	5.x and greater	ASP	Syslog	9.1 and greater
ZeroFOX	ZeroFOX (ASP)	Application	All	ASP	Syslog	9.2 and greater



McAfee. Part of Intel Security.
 2821 Mission College Boulevard
 Santa Clara, CA 95054
 888 847 8766
www.intelsecurity.com

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2014 McAfee, Inc.