McAfee SIEM Device Support

By Vendor

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
A10 Networks	Load Balancer (AX Series)	Load Balancer	All	ASP – Syslog
Adtran	NetVanta	Network Switches & Routers	All	ASP – Syslog
Airdefense	Airdefense	Network Switches & Routers	WIPS Alerts	Java Parser - Syslog
Airtight Interactive	Airtight Interactive	Applications	N/A	ASP – Syslog
Alcatel-Lucent	InfoExpress CyberGatekeeper LAN	Authentication / Network Switches & Routers	ALLOW, DENY, EXIT, CGATE type only	Java Parser - Syslog UDP
	VitalQIP	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP
Apache Software Foundation	Apache	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	Access Logs only	Java Parser - Local files; syslog UDP
	Apache	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	Access, Error and ModSecurity Logs	ASP - Syslog
Arbor	Arbor Peakflow DoS/SP	Network Switches & Routers	Access, Error and ModSecurity Logs	Java Parser - Syslog UDP
	Arbor Peakflow X	Network Switches & Routers	Network Behavior Alerts	Java Parser - Syslog UDP
	Arbor Peakflow X	Network Switches & Routers	Network Behavior Alerts	ASP - Syslog UDP
Aruba	Aruba	Wireless Access Points	N/A	Custom Aruba Parser
Barracuda	Barracuda SPAM Filter	Security Appliances / UTMs	Barracuda SPAM Filter Messages	ASP - Syslog UDP
	Barracuda Web Security Gateways	Security Appliances / UTMs	Barracuda Web Filter Messages	ASP - Syslog UDP
Bit9	Bit9 Parity Suite	Applications	All	CEF
Blue Coat	Blue Coat SG Series	Web Content / Filtering / Proxies	Proxy and System Log	Java Parser - Syslog TCP
	Blue Coat SG Series	Web Content / Filtering / Proxies	Access Log	ASP – Syslog UDP
Blue Lance	BlueLance LT Auditor + for Novell Netware	Applications	Netware Auditing	Java Parser - SQL Server database (TCP port 1433)

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Blue Martini	Blue Martini	Application	All	Code Based
Blue Ridge	BoarderGuard 5000 & 6000 Series		All	ASP - Syslog UDP
Bradford	Bradford Campus Manager	NAC / Network Switches & Routers	All	ASP – Syslog
Brocade	Foundry BigIron, FastIron and NetIron	Network Switches & Routers	Foundary Syslog Messages	ASP - Syslog UDP
	IronView Network Manager	NAC / Network Switches & Routers	All	ASP – Syslog
CA	CA Datacom	Mainframe		Nitro Plugin Protocol
	Identity & Access Management	IAM / IDM	All	Nitro Plugin Protocol
Check Point	Check Point Edge W32 & WU	Firewall	N/A	OPSEC
	Check Point Enterprise & Enterprise Pro	Firewall	N/A	OPSEC
	Check Point Express	Firewall	N/A	OPSEC
	Check Point FW-1 Limited	Firewall	N/A	OPSEC
	Check Point FW1, NG, NGX Standard	Firewall	N/A	OPSEC
	Check Point Smart Center Enterprise Pro	Firewall	N/A	OPSEC
	Check Point IPS-1 Sensory (formerly Network Flight Recorder)	IDS / IPS	NFR Alerts	Nitro Plugin Protocol
	Check Point HA VPN-1	Virtual Private Networks	N/A	OPSEC
	Check Point VPN Pro	Virtual Private Networks	N/A	OPSEC
	Check Point VPN-1 Edge	Virtual Private Networks	N/A	OPSEC
	Check Point VPN-1 Express	Virtual Private Networks	N/A	OPSEC
	SmartEvent	Firewall	All	OPSEC

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Cisco	Cisco CSS (Content Services Switches)	Other	N/A	ASP - Syslog UDP
	Cisco SDEE	Application Protocol	N/A	ASP - SDEE
	TACACS+	Authentication	N/A	ASP – Syslog
	TACPlus	Authentication	Tacplus messages	Java Parser – Syslog UDP
	Cisco ASA	Firewall	%ASA messages	Java Parser - Syslog UDP
	Cisco ASA	Firewall	ASA messages	ASP – Syslog UDP
	Cisco EAP		N/A	Java Parser - Syslog UDP
	Cisco Firewall & Service Module	Firewall	FWSM messages	Java Parser - Syslog UDP
	Cisco PIX	Firewall	PIX messages	Java Parser - Syslog UDP
	Cisco PIX IDS	Firewall / IDS / IPS	IDS messages only	Java Parser - Syslog UDP
	Cisco PIX and PIX IDS	Firewall / IDS / IPS	PIX and IDS messages	ASP – Syslog UDP
	Cisco IOS ACL, IOS FW, IOS IDS	Firewall / IDS / IPS / Network Switches & Routers	%SEC, %FW only, %IDS only	ASP - Syslog UDP
	Cisco IOS Firewall	Firewall / Network Switches & Routers	%FW only	Java Parser - Syslog UDP
	Cisco CSA	Host / Server / Operating System / IDS / IPS	CSA Events	SQL/Text Parser
	CATOS	Host / Server / Operating Systems / Network Switches & Routers	%(CONTROLLER|LINK|OSPF|LINEPROTO|DVLAN|FILESYS|IP|MGMT|SECURITY|SYS|SEC|NTT|Login|FW|Parser) Messages	Java Parser - Syslog UDP
	CATOS	Host / Server / Operating Systems / Network Switches & Routers	%(CONTROLLER|LINK|OSPF|LINEPROTO|DVLAN|FILESYS|IP|MGMT|SECURITY|SYS|SEC|NTT|Login|FW|Parser) Messages	ASP - Syslog UDP
	Cisco ACS	IDS / IPS	Failed/Passed/Radius Accounting/TACACS Accounting & Administration	ASP –Syslog UDP
	Cisco Guard	IDS / IPS	N/A	ASP – Syslog UDP
	Cisco IDS	IDS / IPS	IDS messages only	SDEE
	Cisco IDSM	IDS / IPS	N/A	SDEE
	Cisco IPS	IDS / IPS	N/A	SDEE
	Cisco IOS IDS	IDS / IPS / Network Switches & Routers	%IDS only	ASP - Syslog UDP
	Cisco IOS IPS	IDS / IPS / Network Switches & Routers	IPS Alerts, DUAL, PFINIT-SP, HSRP	ASP - Syslog UDP

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Cisco	Cisco NAC Appliance (Clean Access)	NAC / Network Switches & Routers	All	ASP – Syslog
	Cisco NAC Appliance (Clean Access)	NAC / Network Switches & Routers	NAC Only	Java Parser - HTTP based reques
	NetFlow (Generic)	Network Flow Collection	N/A	ASP - Nitro Netflow Collector
	NX-OS (Nexus)	IDS / IPS / Network Switches & Routers	Aaa, Arp, Auth, Authpriv, cert-enroll, dhcp_snoop, fs-daemon, Fspf, ftp, Fwm, Im, interface-vlan, Ip, Ipconf, Ipqos, Kernel, m2rib, Mail, Mfdm, Mfwd, Ntp, Port, port-channel, port-resources, Provision, Radius, Security, Snmpd, Sifmgr, spanning-tree, Syslog, Sysmgr, TACACS, TACACS+, Track, User, Uucp, vlan_mgr and zone	ASP – Syslog
	Cisco IOS ACL	Network Switches & Routers	%SEC only	Java Parser - Syslog UDP
	Cisco Wireless LAN Controllers	Network Switches & Routers	N/A	ASP – Syslog
	Cisco MARS	Security Management	Incident Notification XMLs	Java Parser - Email (SMTP)
	Cisco VPN Concentrator	Virtual Private Networks	VPN messages	Java Parser - Syslog UDP
	Cisco VSM (VPN Switch Blade)	Virtual Private Networks	VPN messages	Java Parser - Syslog UDP
	Cisco Content Engine	Web Content / Filtering / Proxies	Proxy Logs	Java Parser - FTP Server on Receiver
	Cisco IronPort	Web Content / Filtering / Proxies	IronPort Syslog and Access Messages	ASP - Syslog
Citrix	Citrix Secure Access Gateway	Applications	N/A	ASP – Syslog
	Citrix NetScaler	Web Content / Filtering / Proxies	All	ASP – Syslog
	Citrix NetScaler Web	Web Content / Filtering / Proxies	All	ASP – Syslog
Cluster Labs	Pacemaker CRMD	Applications	All	ASP-Syslog
Cooper Power Systems	Cybectec	Network Switches & Routers	All	ASP – Syslog
	Yukon IMS	Applications	All	ASP-Syslog
CoreTrace	CoreTrace	Applications	Bouncer Messages	ASP – Syslog
CyberGuard	CyberGuard (includes FS, SG, SL)	Firewall	FW messages	Java Parser - Syslog UDP
Cyber-Ark	Enterprise Password Vault	Applications	All	ASP – Syslog

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Dell	PowerConnect	Network Switches & Routers	All	ASP – Syslog
EdgeWave	iPrism Web Security	Web Content / Filtering / Proxies	All	ASP – Syslog
eEye	eEye Retina	Vulnerability Systems	Vulnerability Assessment data support	N/A
	eEye Retina Enterprise Manager	Vulnerability Systems	Vulnerability Assessment data support	N/A
Enterasys	Enterasys Dragon Sensor/Squire	IDS / IPS	NIDS and HIDS Messages	Java Parser - MySQL database (T connection)
	N Series Switches	Network Switches & Routers	All	ASP – Syslog
	NAC	NAC/Network Switches & Routers	All	ASP – Syslog
	S Series Switches	Network Switches & Routers	All	ASP – Syslog
Extreme Networks	ExtremeWare XOS	NAC/Network Switches & Routers	All	ASP – Syslog
F5	Access Policy Manager (APM)	NAC/Network Switches & Routers	All	ASP – Syslog
	Application Security Manager (ASM)	Web Content / Filtering / Proxies	N/A	Nitro Plugin Protocol
	FirePass SSL VPN	Virtual Private Network	All	ASP – Syslog
	Local Traffic Manager	Web Content / Filtering / Proxies	All	ASP - Syslog UDP
Fairwarning	Fairwarning Privacy Monitoring	Application Security	N/A	Nitro Plugin Protocol
FireEye	FireEye Malware Protection	Antivirus/Malware	N/A	CEF Parser
Fluke Networks	AirMagnet Enterprise	Network Switches & Routers	All	ASP – Syslog
Force10 Networks	FTOS	Network Routers & Switches	All	ASP – Syslog
ForeScout	CounterACT	NAC/Network & Switches	All	ASP – Syslog
Fortinet	Fortinet Fortigate	Firewall	IPS , webfilter, spamfilter, event, traffic type messages	Java Parser - Syslog
	Fortinet Fortigate	Firewall	IPS , webfilter, spamfilter, event, traffic type messages	ASP - Syslog
	Fortinet WAF	Firewall	All	ASP – Syslog
FreeRadius	FreeRadius	Authentication	AUTH	ASP – Syslog
Funkwerk	PacketAlarm IPS	IDS / IPS	IPS Alerts	Java Parser - Syslog UDP
GTA	GNAT	Firewall	All	ASP – Syslog

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
HP	HP-UX (Hewlett-Packard)	Host / Server / Operating Systems	ssh/telnet/ftp/rsh/inetd/sendmail/syslogd/su	Java Parser - Syslog UDP
	LaserJet	Printers	All	ASP – Syslog
	OpenVMS	Operating Systems	N/A	ASP - Syslog
	HP ProCurve	Network Switches & Routers	Procurve Syslog Messages	ASP - Syslog UDP
Infoblox	NIOS	Applications	All	ASP – Syslog
IBM	Guardium	Database Activity Monitoring	All	ASP – Syslog UDP
I	System Z DB2	Database	N/A	DBM Agent - 7.1.x, 8.x, 9.x
	System Z DB2	Database	All Versions	BSafe Agent
	ISS Real Secure Server Sensor	Host / Server / Operating Systems	RealSecure Network /Server Sensor, Proventia A/G/M Series Applicances	Java Parser - SQL Server databas (TCP port 1433)
	IBM AIX OS	Host / Server / Operating Systems	ssh/telnet/ftp/rsh/inetd/sendmail/syslogd/su	Java Parser - Syslog UDP
	ISS Desktop Protector	Host / Server / Operating Systems / Other	BlackICE and Desktop Protection System	Java Parser - SQL Server databas (TCP port 1433)
	ISS Real Secure Network Sensor	Other	RealSecure Network /Server Sensor, Proventia A/G/M Series Applicances	Java Parser - SQL Server databas (TCP port 1433)
	ISS Site Protector	Security Management	RealSecure Network /Server Sensor, Proventia A/G/M Series Applicances	Custom Text Parser
	z/OS, z/vm	Mainframe	SMF (System Management Facilities) Types 30, 14, 15, 17, 18, 56, 62, 64, 80	Nitro Plugin Protocol
	Tivoli Access Manager for Operating Systems	Authentication	All	Nitro Plugin Protocol
	Tivoli Identity & Access Manager	IAM / IDM	All	Nitro Plugin Protocol
	z/OS, z/VM	Mainframe	RACF (Resource Access Control Facility	Nitro Plugin Protocol
	Informix	Database	N/A	
Imperva	Database Activity Monitor	Database	All	Code Based
	Web Application Firewall	Firewall	All	Code Based
Intersect Alliance	SNARE	Other	Snare for Windows, Snare for AIX	ASP - Syslog UDP

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
IP Fix	IP Fix	Network Flow Collection		Custom
iTron	iTron Enter	Smart Grid Application	All	ASP – Syslog
Juniper	Juniper Netscreen Firewall	Firewall	System and Traffic notification messages	Java Parser - Syslog UDP OR AS Syslog
	Juniper Netscreen IDP	IDS / IPS	4.x via NSM	Java Parser - Syslog UDP OR AS Syslog
	Juniper Netscreen Security Manager	Network Switches & Routers	IDP, FW	Java Parser - Syslog UDP
	NSM	Applications / Host / Server / Operating Systems	All	ASP
	Juniper Routers (JunOS)	Network Switches & Routers	JunOS Messages	ASP - Syslog UDP
	Juniper Secure Access SSL VPN	Virtual Private Networks	Log/Monitoring Events	ASP- Syslog UDP
	SRX	Firewall/VPN	JunOs Messages	ASP –Syslog UDP
Kaspersky	Admin Console	Antivirus	All anti-virus events through the console	Windows Agent
KEMP Technologies	LoadMaster	Network Switches & Routers	All	ASP – Syslog
Lancope	Lancope Stealth Watch	IDS / IPS / Network Switches & Routers	Stealth Watch messages only	Java Parser - Syslog UDP
	Lancope Stealth Watch	IDS / IPS / Network Switches & Routers	All	ASP - Syslog
LINUX	LINUX	Host / Server / Operating Systems	AuditD, BIND, Netfilter, ProFTPD, Samba, Open SSH, Pure FTPD, cron, exinit	ASP – Syslog
Lumension	PatchLink Scan	Vulnerability Systems	Vulnerability Assessment data support	N/A
Macintosh	OS-X Server & Workstation	Applications / Security Management / Host / Server / Operating Systems	Server and Workstation	ASP - Syslog
MailGate, Ltd.	MailGate Server	Applications / Security Management / Host / Server / Operating Systems	All	ASP – Syslog
Mainframe	DB2	Host / Server / Operating Systems	All	Bsafe Agent
Mainframe	IMS	Host / Server / Operating Systems	All	Bsafe Agent
Mainframe	SMF DB2	Host / Server / Operating Systems	All	Bsafe Agent
Mainframe	SMF RACF	Host / Server / Operating Systems	All	Bsafe Agent
Mainframe	SMF FTP & Telnet	Host / Server / Operating Systems	All	Bsafe Agent
Mainframe	SMF VSAM	Host / Server / Operating Systems	All	Bsafe Agent

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Mainframe	Top Secret, Type 80 SMA_RT	Host / Server / Operating Systems	ICH/IEF/SMF/TSS messages	Java Parser – Syslog UDP
McAfee	McAfee Antivirus	AntiVirus	N/A	WMI Parser – WMI
	McAfee ePolicy Orchestrator (EPO)	Applications / Security Management / Host / Server / Operating Systems	AV/HIPS/Host FW messages	Java Parser - SQL Server databas (TCP port 1433)
	McAfee AntiSpyware (ASE), Data Loss Prevention (DLP), ePolicy Orchestrator Agent [Common McAfee Framework Agent] (CMA), GroupShield for Domino (GSD), GroupS for Exchange (GSE), McAfee Host Intrusion Prevention (HIPS), McAfee Network Access Control (MNAC), McAfee Policy Auditor (PAE), McAfee SiteAdvisor (SAE), McAfee VirusScan (VSE), SolidCore (SCOR)			
	Firewall Enterprise	Firewall / IDS / IPS	All	ASP – Syslog
	Firewall Enterprise	Firewall / IDS / IPS	FW Logs Only	Java Parser - Syslog UDP
	Email and Web Security	Web Content / Filtering / Proxies	All	CEF
	Email and Web Security	Web Content / Filtering / Proxies	All	ASP - Syslog
	McAfee HIPS	IDS / IPS	HIPS data through ePO for HIPS 6.0 and above	Java Parser - Entercept API till 5.x ePO SQL Server database for 6.0
	Network Security (formerly IntruShield)	IDS / IPS	IPS Alerts	Java Parser - Syslog UDP
	Network Security (formerly IntruShield)	IDS / IPS	IPS Alerts	ASP - Syslog
	Vulnerability Manager	Vulnerability Systems	Vulnerability Assessment data support	N/A
	Web Gateway	Web Content / Filtering / Proxies	All	ASP – Syslog
	McAfee WebShield SMTP	Web Content / Filtering / Proxies	Webshield Syslog Messages	ASP - Syslog UDP
Microsoft	Exchange	Applications / Host / Server / Operating Systems	Message Tracking Logs	ASP - Windows Agent
	Forefront Threat Management Gateway	IDS/IPS	All	Code Based
	Microsoft Windows	Applications / Host / Server / Operating Systems	System, Security, Application, DNS, DHCP and File Replication.	WMI Parser – WMI
	Microsoft Windows	Server	Debug DNS Logs (file)	ASP – Windows Agent
	Microsoft Windows	Server	Debug DHCP Logs (file)	ASP – Windows Agent
	Microsoft SQL Server	Database	N/A	WMI Parser – WMI
	Microsoft SQL Server	Database	N/A	DBM Agent - MSSQL 2000 (SP4), 2005, 2008
	Microsoft ISA Server	Firewall / Host / Server / Operating Systems / Web Content / Filtering / Proxies / Virtual Private Networks	N/A	WMI Parser – WMI
	Microsoft Operations Manager	Host / Server / Operating Systems	MOM Messages	Java Parser - SQL Server databas (TCP port 1433)

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Microsoft	Microsoft IIS	Host / Server / Operating Systems / Web Content / Filtering / Proxies	IIS web traffic logs in W3C format	Java Parsing Agent - Local Files; syslog using Snare
	Microsoft IIS	Host / Server / Operating Systems / Web Content / Filtering / Proxies	IIS web traffic logs in W3C format	Windows Agent
	Microsoft Exchange Server	Other	N/A	WMI Parser – WMI
	Microsoft Active Directory	Other	N/A	WMI Parser – WMI
	Microsoft SCOM	Security Management	2007	Nitro Plugin Parser
Mirage Networks	Mirage Counterpoint	NAC / Network Switches & Routers	Threat and Response Messages	Java Parser - Syslog UDP
nCircle	IP360 Scanner	Vulnerability Systems	Vulnerability Assessment data support	N/A
Nessus	Nessus	Vulnerability Systems	Vulnerability Assessment Data Support	N/A
NetApp	DataFort	Storage Switch	All	ASP – Syslog
	Data OnTap	Storage	OnTap Logs – audit, message, sis and snapmirror logs	ASP – Windows Agent
	FAS	Storage	.evt files	Windows Agent
Netfort Technologies	Netfort LANGuardian	Applications / Security Management / Host / Server / Operating Systems	All	ASP – Syslog
netIQ	netIQ Security Manager	Network Switches & Routers / Security Management	netIQ Alerts	Java Parser - SQL Server databas (TCP port 1433)
NetWitness	NextGen	Application Protocol	N/A	CEF Parser
	Spectrum	Malware	All	URL Integration
NitroSecurity	NitroView DBM	Database	N/A	ASP - Syslog
	NitroSecurity IPS	Firewall / IDS / IPS / Network Switches & Routers	N/A	ASP - Syslog
	Nitro Plug-in Protocol	Other	N/A	Nitro Plugin Protocol
	NitroSecurity SNMP	Other	N/A	SNMP
Nokia	Nokia IPSO	Firewall	IPSO OS logs	Java Parser - Syslog UDP
Nortel	Passport 8000	Network Switches & Routers	All	ASP – Syslog
	VPN Gateway 3050	Virtual Private Networks	All	ASP
Oracle	MySQL	Database	N/A	Yes, 4.1.22.x, 5.0.3x
	Oracle Common Audit	Database	System	Java Parser Agent - Local Files
	Oracle Fine-Grained Audit	Database	Fine Grained Audits	Java Parser - DB Audit Tables through JDBC

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Oracle	Oracle	Database	N/A	DBM Agent - Oracle 8.0.3+, 9.x, 1 11.x
	Identity & Access Manager	IAM / IDM	All	Nitro Plugin Protocol
Osiris	Host Integrity Monitoring	Host / Server / Operating System / IDS / IPS	ISAKMP, RADIUS, SECURITY, Accounting, RIP, VR messages only	ASP – Syslog
Palo Alto	PA-2000, 4000, 500	Firewall	ALL	ASP - Syslog
Patrick Townsend	AS-400	Host	All	CEF Parser
Peoplesoft	Peoplesoft	Applications	N/A	Nitro Plugin Protocol
PostFix	PostFix	Applications	All	ASP-Syslog
PostgreSQL	PostgreSQL	Database	All	ASP
Powertech	AS-400	Host	All	CEF Parser
ProofPoint	Messaging Security Gateway	Applications	All	ASP
Qualys	QualysGuard	Vulnerability Systems	Vulnerability Assessment Data Support	N/A
Quest	ChangeAuditor for Active Directory	Applications	All	ASP – WMI
Radware	DefensePro	IDS / IPS	DefensePro Alerts	Java Parser - Syslog UDP
	FireProof and LinkProof	Network Switches & Routers	All	ASP – Syslog
Rapid 7	MetaSploit Pro	Penetration Testing	All	Custom
	Nexpose VA Scanner	Vulnerability Systems	Vulnerability Assessment Data Support	N/A
Red Hat	Red Hat Linux OS Events	Host / Server / Operating Systems	ssh/telnet/ftp/rsh/inetd/sendmail/syslogd/su/pam unix/rhosts/xinetd	Java Parser - Syslog UDP
Riverbed	Steelhead	Security Appliances / UTMs	All	ASP – Syslog
RSA	RSA Authentication Manager (windows)	Authentication	N/A	WMI Parser – WMI
	RSA Authentication Manager (UNIX)	Authentication	ACE Server Logs Only	Java Parser - Unix Syslog
	RSA Authenticaiton Manager (Windows & UNIX)	Authentication	All	ASP – Syslog

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
SafeNet	Safenet HSM	Application Security	N/A	ASP – Syslog
Saint	Saint Vulnerability Scanner	Vulnerability Systems	Vulnerability Assessment data support	N/A
Savant	Savant Protection	Anti-Malware	All	CEF
SecureAuth	SecureAuth IEP	Authentication	All	ASP – Syslog
Secure Crossing	Secure Crossing ZenWall	Applications / Security Management / Host / Server / Operating Systems	All	ASP – Syslog
sFlow	sFlow (Generic)	Network Flow Collection	N/A	Nitro sFlow Collector
Silver Spring Networks	Access and Endponts	Smart Grid	All	ASP – Syslog
SonicWALL	Aventail	Virtual Private Networks	VPN messages	ASP
	SonicWALL FW	Firewall	FW/IPS/VPN	ASP - Syslog
Sophos	Sophos Email Security & Data Protection	Web Content / Filtering / Proxies	All	ASP
	Sophos Enterprise Console	Antivirus/HIDS	All AV and endpoint events from the console	Nitro Plugin Protocol
	Web Security & Control	Web Content / Filtering / Proxies	All	ASP - Syslog
Sourcefire	Snort NIDS	IDS / IPS	IDS messages only	Java Parser - Syslog UDP
	Sourcefire Intrusion Sensor	IDS / IPS	IDS messages only(eStreamer)	Java Parser - Estreamer API usin TCP port 8302
	Sourcefire NS/RNA	IDS/IPS	IDS messages only(eStreamer)	ASP - Syslog UDP
Squid	Squid Web Proxy	Web Content / Filtering / Proxies	Web Proxy Logs	Java Parser – N/A
	Squid Web Proxy	Web Content / Filtering / Proxies	Web Proxy Logs	ASP – Syslog
StillSecure	Strata Guard	Firewall / Security Management / IDS / IPS / Virtual Private Networks	Firewall Events	ASP – Sylosg
Stonesoft	Stonesoft Stonegate Management Center	Firewall / Security Management / IDS / IPS / Virtual Private Networks	IPS/FW/VPN	Java Parser – Syslog UDP
	Stonesoft Stonegate Firewall /VPN	Firewall / Virtual Private Networks	FW/VPN activities	Java Parser – Syslog UDP
	Stonesoft Stonegate IPS	IDS / IPS	IPS Alerts	Java Parser – Syslog UDP
Sun	Solaris BSM	Host / Server / Operating Systems	BSM Audit Logs	Java Parser - Syslog UDP
	Solaris OS Events	Host / Server / Operating Systems	ssh/telnet/ftp/rsh/inetd/sendmail/syslogd/su/xinetd	Java Parser - Syslog UDP
	iPlanet	Web Content / Filtering / Proxies	N/A	Java Parser - Syslog UDP
Sybase	Sybase	Database	N/A	DBM Agent - 11.x, 12.x, 15.x

Vendor	Device Name	Device Type	Supported Logs	Parser *Method of Collection*
Symantec	Symantec Anti Virus	AntiVirus	N/A	WMI Parser – WMI
	Symantec AV CE Server	Antivirus	All	NPP
	Symantec Endpoint Protection	AntiVirus	Host FW/IPS/AV/Control/NAC messages	Java Parser – Syslog UDP
	Symantec Endpoint Protection	AntiVirus	Host FW/IPS/AV/Control/NAC messages	ASP – Syslog
	Symantec Intruder Alert	Host / Server / Operating Systems	ITA Alerts	Java Parser – Syslog UDP
	Symantec Critical System Protection	IDS / IPS	Events and Audit messages	Java Parser – SQL Server database (TC port 1433)
	Symantec ManHunt	IDS / IPS	IDS messages only	Java Parser – Syslog UDP
	Symantec HIDS	IDS / IPS / Other	HIDS messages	Java Parser – DB2 database
	PGP Universal Server	Host / Server / Operating Systems	All	All
	Symantec Web Gateway	Web Content / Filtering / Proxies	All messages	ASP – Syslog
System i	System i	Host / Server / Operating Systems	All	BSafe Agent
TippingPoint	Tippingpoint Unitity One	IDS / IPS	N/A	ASP – Syslog
	Tippingpoint SMS Format	Security Management	IDS messages	Java Parser – Syslog UDP
	Tippingpoint SMS Format	Security Management	IDS messages	ASP - Syslog
Tofino	Firewall LSM	Firewall / Virtual Private Networks	All	ASP – Syslog
Top Layer	TopLayer Attack Mitigator	IDS / IPS	N/A	ASP – Syslog
Trend Micro	Control Manager (IMSS & IWSS)	AntiVirus / Vulnerability Systems	IMSS and IWSS	Java Parser – SQL Server database (TCP port 14
	Deep Security IDS	HIDS	HIDS and Windows messages	ASP - Syslog
	OSSEC	FIM/HIDS	All	ASP – Syslog
Tripwire	Enterprise	Database / Security Management	Tripwire Integrity Check messages	Java Parser – Syslog UDP
	Tripwire NIDS	IDS / IPS / Other	N/A	SNMP
Trustvave	NAC	NAC	All NAC events	ASP – Syslog
	Vericept	DLP	All	CEF
	Webdefend	Web Content / Filtering / Proxies	All	ASP – Syslog
Type 80	Type 80 SMA_RT	Host / Server / Operating Systems	ICH/IEF/SMF/TSS messages	Java Parser – Syslog UDP
VMWare/EMC	VMWare ESX/ESX i	Applications	Virtual System logs	ASP - Syslog
Vormetric	Data Security	Applications	All	ASP – Syslog
WatchGuard	WatchGuard Firebox	Firewall	All	ASP – Syslog
Websense	Websense Enterprise	Web Content / Filtering / Proxies	Web Security and Filtering Messages	Java Parser – SQL Server databa (TCP port 1433)
Xirrus	802.11abgn WiFi Arrays	Switches & Routers	All	ASP – Syslog
Zonelabs	Zonelabs Integrity	Firewall	N/A	Java Parser – SQL Data Source