

Product Name	Device Type	Vendor	Collection Method
Adapter (generic)	Database	LogMatrix	JDBC
Adapter (generic)	Any	LogMatrix	Syslog
Adapter (generic)	Any	LogMatrix	Log File (tailing a file)
Adapter (generic)	Any	LogMatrix	Batch Log File (scheduled batches of files)
Adapter (generic)	Any	LogMatrix	Streaming (listens for connections/data over UDP or TCP from any source)
Adapter (generic)	Any	LogMatrix	SNMP (receives traps)
Adapter (generic)	Any	LogMatrix	CheckPoint LEA
Adapter (generic)	Any	LogMatrix	WinWatch
Apache	WS	Apache Software	
Arbor PeakFlow SP	AD	Arbor Networks	SNMP
Arbor PeakFlowX	AD	Arbor Networks	SNMP
Bluecoat SG	CM	Bluecoat Systems	Local log adapter
BorderWare	AV	WatchGuard	Syslog
Checkpoint Firewall	FW	Check Point	lea_client exe
Cisco ACS (Active Control Server)	AAA	Cisco	ciscoacs exe
Cisco ASA FW	UTM	Cisco	Syslog
Cisco Content Services Switch	LB	Cisco	Syslog
Cisco Firewall	FW	Cisco	Syslog
Cisco Guard DDoS	AD	Cisco	Syslog
Cisco IDS/IPS	NIDS	Cisco	OCiscoSDEEAdapter
Cisco Routers/Switches	RS	Cisco	Syslog
Cisco Security Agent	HIDS	Cisco	OSICSA exe
Cisco VPN	VPN	Cisco	NONE
CommandCenter	PC	LogMatrix	log
Cyberguard Firewall	FW	McAfee	Syslog
eEye Blink	IPS	eEye Digital Security	OSleEye_Blink exe
Enterasys Dragon	NIDS	Enterasys	DB adapter
Fortinet FortiGate	CM	Fortinet	Syslog
Fortinet Fortigate FW	FW	Fortinet	Syslog or SNMP
IBM AIX	OS	IBM	Syslog
IBM AS400/iSeries	OS	IBM	OAS400Adapter
IBM SiteProtector	NIDS	IBM	DB adapter
Interwoven	CM	Autonomy	DB adapter
Juniper Netscreen Firewall	FW	Juniper Networks	Syslog
Juniper Netscreen IDP	IDP	Juniper Networks	Syslog
Lancope StealthWatch	AD	Lancope	NONE
Lucent Firewall Brick	FW	Alcatel-Lucent	lucentlogreader exe
Mazu Enforcer	AD	Riverbed Cascade	SNMP
Mazu Profiler	AD	Riverbed Cascade	SNMP
McAfee ePolicy Orchestrator	AV	McAfee	DB adapter

McAfee IntruShield	NIDS	McAfee	Syslog
Microsoft Active Directory	AAA	Microsoft	WinWatch exe
Microsoft ISA Firewall	FW	Microsoft	OSIMicrosoftISA exe
nCircle Threat Monitor	NIDS	nCircle	NONE
NerveCenter	NerveCenter	LogMatrix	NONE
NerveCenter Inform	NerveCenter	LogMatrix	SNMP Inform
Nortel VPN	VPN	Nortel	NONE
OpenVMS	OS	HP	Syslog
Osiris Host Integrity Monitor	HIDS	OSIRIS	Syslog
PowerTech Interact	HIDS	PowerTech	Syslog
QualysGuard	VA	Qualys	qg-export exe
Red Hat Linux	OS	RedHat	Syslog
RSA SecureID	AAA	RSA Security	Syslog
SecureComputing Firewall	FW	McAfee	Syslog
SecureNet Provider	NIDS	Intrusion	OSISecureNet exe
Smoothwall FW/IDS	UTM	SmoothWall	Syslog
Snort IDS	NIDS	Open Source	Syslog
Snort Preprocessors	NIDS	Open Source	Syslog
Solaris	OS	Oracle - Sun	Syslog
Sophos Antivirus	AV	Sophos	SNMP
SourceFire Defense Center	NIDS	Sourcefire	OSourceFireAdapter
Sun Java Core Logging	LOGGING	Oracle - Sun	Local log adapter
Sun Solaris IPFilters FW	FW	Oracle - Sun	OSISolaris10 exe
Symantec AV Corporate	AV	Symantec	OSISymantecAV exe
Symantec Enterprise Firewall	FW	Symantec	remotelogfile exe
Symantec Manhunt	NIDS	Symantec	Syslog
Thompson Elite	CM	Thompson	DB adapter
TopLayer Attack Mitigator	IPS	TopLayer	Syslog
Trend Micro IMSS	CM	Trend Micro	OSITrendIMSS
Trend Micro OfficeScan	AV	Trend Micro	Local log adapter
Tripwire	HIDS	Tripwire Inc.	Syslog/WinWatch
UnityOne IPS	IPS	TippingPoint	OSITippingPoint exe
Websense	CM	WEBSense	NONE

Device Types

AAA - Authentication, Authorization & Accounting

AD - Active Directory

AV - Anti-Virus/Anti-Malware

CM - Content Management

FW - Firewall

HIDS - Host Intrusion Detection System

IPS - Intrusion Protection System

LB - Load Balancer

NIDS - Network Intrusion Detection System

OS - Operating System

RS - Routers & Switches

UTM - Unified Threat Management

VA - Vulnerability Assessment

VPN - Virtual Private Network

WS - Web Server