QRadar supported DSMs

Contents

QRadar supported DSMs

IBM® Security QRadar® can collect events from your third-party security products by using a plugin file that is called a Device Support Module (DSM). QRadar supports an extensive list of third-party security solutions.

If your device or appliance is not listed, contact your sales representative.

Table 1. QRadar Supported DSMs

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
3Com	8800 Series Switch v3.01.30	Syslog	Status and network condition events	Yes	No	No
Amazon	Amazon AWS CloudTrail v1.0	Log File	All events	No	Yes	No
Ambiron	TrustWave ipAngel v4.0	Syslog	Snort-based events	No	No	No
Apache	HTTP Server v1.3 and later	Syslog	HTTP status	Yes	No	No
APC	UPS	Syslog	Smart-UPS series events	No	No	No
Apple	Mac OS X (10)	Syslog	Firewall, web server (access/ error), privilege, and information events	No	Yes	No
Application Security, Inc.	DbProtect v6.2, v6.3, v6.3sp1, v6.3.1, and v6.4	Syslog	All events	Yes	No	No
Arbor Networks	Pravail APS	Syslog	All events	Yes	No	No
Arpeggio Software	SIFT-IT v3.1 and later	Syslog	All events configured in the SIFT-IT rule set	Yes	No	No
Array Networks	SSL VPN ArraySP v7.3	Syslog	All events	No	Yes	Yes
Aruba Networks	Mobility Controllers v2.5 and later	Syslog	All events	Yes	No	No
Avaya Inc.	Avaya VPN Gateway v9.0.7.2	Syslog	All events	Yes	Yes	No
BalaBit IT Security	Microsoft Windows Security Event Log v4.x	Syslog	Microsoft Event Log Events	Yes	Yes	No
BalaBit IT Security	Microsoft ISA v4.x	Syslog	Microsoft Event Log Events	Yes	Yes	No
Barracuda Networks	Spam & Virus Firewall v5.x and later	Syslog	All events	Yes	No	No
Barracuda Networks	Web Application Firewall v7.0.x	Syslog	System, web firewall, access, and audit events	Yes	No	No
Barracuda Networks	Web Filter 6.0.x and later	Syslog	Web traffic and web interface events	Yes	No	No
Bit9	Security Platform v6.0.2 and later	Syslog	All events	Yes	Yes	No
BlueCat Networks	Adonis v6.7.1-P2 and later	Syslog	DNS and DHCP events	Yes	No	No
Blue Coat	SG v4.x and later	Syslog Log File Protocol	All events	No	No	Yes
Bridgewater Systems	AAA v8.2c1	Syslog	All events	Yes	Yes	No
Brocade	Fabric OS V7.x	Syslog	System and audit events	Yes	No	No
CA	Access Control Facility v12 to v15	Log File Protocol	All events	No	No	Yes
CA	SiteMinder	Syslog	All events	No	No	No
CA	Top Secret v12 to v15	Log File Protocol	All events	No	No	Yes

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Check Point	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	Syslog or OPSEC LEA	All events	Yes	Yes	Yes
Check Point	VPN-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77 NGX	Syslog or OPSEC LEA	All events	Yes	Yes	No
Check Point	Provider-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX	Syslog or OPSEC LEA	All events	Yes	Yes	No
Cilasoft	Cilasoft QJRN/400 V5.14.K and later	Syslog	IBM audit events	Yes	Yes	No
Cisco	4400 Series Wireless LAN Controller v7.2	Syslog or SNMPv2	All events	No	No	No
Cisco	CallManager v8.x	Syslog	Application events	Yes	No	No
Cisco	ACS v4.1 and later if directly from ACS v3.x and later if using ALE	Syslog	Failed Access Attempts	Yes	Yes	No
Cisco	Aironet v4.x and later	Syslog	Cisco Emblem Format	Yes	No	No
Cisco	ACE Firewall v12.2	Syslog	All events	Yes	Yes	No
Cisco	ASA v7.x and later	Syslog	All events	Yes	Yes	No
Cisco	ASA v7.x and later	NSEL Protocol	All events	No	No	No
Cisco	CSA v4.x, v5.x and v6.x	Syslog SNMPv1 SNMPv2	All events	Yes	Yes	No
Cisco	CatOS for catalyst systems v7.3 and later	Syslog	All events	Yes	Yes	No
Cisco	IDS/IPS v5.x, v6.x, and v7.2	SDEE	All events	No	No	No
Cisco	IronPort v5.5, v6.5, and v7.1	Syslog, Log File Protocol	All events	No	No	No
Cisco	Firewall Service Module (FWSM) v2.1 and later	Syslog	All events	Yes	Yes	Yes
Cisco	Catalyst Switch IOS, 12.2, 12.5, and later	Syslog	All events	Yes	Yes	No
Cisco	NAC Appliance v4.x and later	Syslog	Audit, error, failure, quarantine, and infected events	No	No	No
Cisco	Nexus v6.x	Syslog	Nexus-OS events	Yes	No	No
Cisco	PIX Firewall v5.x, v6.3, and later	Syslog	Cisco PIX events	Yes	Yes	Yes
Cisco	IOS 12.2, 12.5, and later	Syslog	All events	Yes	Yes	No
Cisco	VPN 3000 Concentrator vVPN 3005, 4.1.7.H	Syslog	All events	Yes	Yes	Yes
Cisco	Wireless Services Modules (WiSM) v 5.1 and later	Syslog	All events	Yes	No	No
Cisco	Identity Services Engine v1.1	UDP Multiline Syslog Protocol	Device events	No	Yes	No
Citrix	NetScaler v9.3 to v10.0	Syslog	All events	Yes	Yes	No
Citrix	Access Gateway v4.5	Syslog	Access, audit, and diagnostic events	Yes	No	No
CRYPTOCard	CRYPTO- Shield v6.3	Syslog	All events	No	No	No
Cyber-Ark	Vault v6.x	Syslog	All events	Yes	Yes	No
CyberGuard	Firewall/VPN KS1000 v5.1	Syslog	CyberGuard events	Yes	No	No
Damballa	Failsafe v5.0.2 and later	Syslog	All events	Yes	No	No
Digital China Networks	DCS and DCRS Series switches v1.8.7 and later	Syslog	DCS and DCRS IPv4 events	No	No	No
DG Technologies	MEAS	LEEF Syslog	Mainframe events	Yes	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Enterasys	800-Series Switch	Syslog	All events	Yes	No	No
Enterasys	Dragon v5.0, 6.x, v7.1, v7.2, v7.3, and v7.4	Syslog SNMPv1 SNMPv3	All relevant Enterasys Dragon events	Yes	No	No
Enterasys	Matrix Router v3.5	Syslog SNMPv1 SNMPv2 SNMPv3	SNMP and syslog login, logout, and login failed events	Yes	No	No
Enterasys	NetSight Automatic Security Manager v3.1.2	Syslog	All events	Yes	No	No
Enterasys	Matrix N/K/S Series Switch v6.x, v7.x	Syslog	All relevant Matrix K-Series, N-Series and S-Series device events	Yes	No	No
Enterasys	Stackable and Standalone Switches	Syslog	All events	Yes	Yes	No
Enterasys	XSR Security Router v7.6.14.0002	Syslog	All events	Yes	No	No
Enterasys	HiGuard Wireless IPS V2R2.0.30	Syslog	All events	Yes	No	No
Enterasys	HiPath Wireless Controller V2R2.0.30	Syslog	All events	Yes	No	No
Enterasys	NAC v3.2 and v3.3	Syslog	All events	Yes	No	No
Extreme Networks	Extreme Ware v7.7 and XOS v12.4.1.x	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP AFM v11.3	Syslog	Network, network DoS, protocol security, DNS, and DNS DoS events	Yes	No	No
F5 Networks	BIG-IP LTM v4.5, v9.x to v11.x	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP ASM v10.2	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP APM v10.x, and v11.x	Syslog	All events	Yes	No	No
F5 Networks	FirePass v7.0	Syslog	All events	Yes	Yes	No
Fair Warning	Fair Warning v2.9.2	Log File Protocol	All events	No	No	No
Fidelis Security Systems	Fidelis XPS 7.3.x	Syslog	Alert events	Yes	No	No
FireEye	CMS, MPS, eMPS and MA v5.1 patch level 5	Syslog	All events	No	Yes	No
ForeScout	CounterACT v7.x and later	Syslog	Denial of Service, system, exploit, authentication, and suspicious events	No	No	No
Fortinet	FortiGate FortiOS v2.5 and later	Syslog	All events	Yes	Yes	Yes
Foundry	FastIron v3.x.x and v4.x.x	Syslog	All events	Yes	Yes	No
Great Bay	Beacon	Syslog	All events	Yes	Yes	No
Great Bay	Beacon	Syslog	All events	Yes	No	No
HBGary	Active Defense v1.2 and later	Syslog	All events	Yes	No	No
HP	Tandem	Log File Protocol	Safe Guard Audit file events	No	No	No
HP	ProCurve K.14.52	Syslog	All events	Yes	No	No
HP	UX v11.x and later	Syslog	All events	No	Yes	No
Honeycomb Technologies	Lexicon File Integrity Monitor mesh service v3.1 and later	Syslog	integrity events	Yes	No	No
Huawei	S Series Switch S5700, S7700, and S9700 using V200R001C00	Syslog	IPv4 events from S5700, S7700, and S9700 Switches	No	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Huawei	AR Series Router (AR150, AR200, AR1200, AR2200, and AR3200 routers using V200R002C00)	Syslog	IPv4 events	No	No	No
IBM	AIX v6.1 and v7.1	Syslog, Log File Protocol	Configured audit events	Yes	No	No
IBM	AIX 5.x, 6.x, and v7.x	Syslog	Authentication and operating system events	Yes	Yes	No
IBM	AS/400 iSeries DSM V5R3 and later	Log File Protocol	All events	No	Yes	No
IBM	AS/400 iSeries - Robert Townsend Security Solutions V5R1 and later	Syslog	CEF formatted messages	Yes	Yes	No
IBM	AS/400 iSeries - Powertech Interact V5R1 and later	Syslog	CEF formatted messages	Yes	Yes	No
IBM	InfoSphere 8.2p45	Syslog	Policy builder events	No	No	No
IBM	ISS Proventia M10 v2.1_2004.1122_15.13.53	SNMP	All events	No	No	No
IBM	Lotus Domino v8.5	SNMP	All events	No	No	No
IBM	Proventia Management SiteProtector v2.0 and v2.9	JDBC	IPS and audit events	No	No	No
IBM	RACF v1.9 to v1.13	Log File Protocol	All events	No	No	Yes
IBM	CICS v3.1 to v4.2	Log File Protocol	All events	No	No	Yes
IBM	DB2 v8.1 to v10.1	Log File Protocol	All events	No	No	Yes
IBM	z/OS v1.9 to v1.13	Log File Protocol	All events	No	No	Yes
IBM	Informix v11	Log File Protocol	All events	No	No	No
IBM	IMS	Log File Protocol	All events	No	No	No
IBM	Security Network Protection (XGS) v5.0 with fixpack 7	Syslog	System, access, and security events	Yes	No	No
IBM	Security Network IPS v4.6 and later	Syslog	Security, health, and system events	Yes	No	No
IBM	Security Identity Manager 6.0.x and later	JDBC	Audit and recertification events	No	Yes	No
IBM	Tivoli Access Manager IBM Web Security Gateway v7.x	Syslog	audit, access, and HTTP events	Yes	Yes	No
IBM	Tivoli Endpoint Manager v8.2.x and later	IBM Tivoli Endpoint Manager SOAP Protocol	Server events	No	Yes	No
IBM	WebSphere Application Server 5.0.x to 6.1	Log File Protocol	All events	No	Yes	No
IBM	zSecure Alert v1.13.x and later	UNIX syslog	Alert events	Yes	Yes	No
IBM	Security Access Manager v8.1 and v8.2	Syslog	Audit, system, and authentication events	Yes	No	No
IBM	Security Directory v6.3.1 and later	Syslog LEEF	All events	Yes	Yes	No
Imperva	SecureSphere v6.2 and v7.x or 9.5 and 10.0 (LEEF)	Syslog	All events	Yes	No	No
Infoblox	NIOS v6.x	Syslog	All events	No	Yes	No
Internet Systems Consortium (ISC)	BIND v9.9	Syslog	All events	Yes	No	No
iT-CUBE	agileSI v1.x	SMB Tail	AgileSI SAP events	No	Yes	No
Itron	Openway Smart Meter	Syslog	All events	Yes	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Juniper Networks	AVT	JDBC	All events	No	No	Yes
Juniper Networks	DDoS Secure	Syslog	All events	Yes	No	No
Juniper Networks	DX	Syslog	Status and network condition events	Yes	No	Yes
Juniper Networks	Infranet Controller v2.1, v3.1 & v4.0	Syslog	All events	No	Yes	Yes
Juniper Networks	Firewall and VPN v5.5r3 and later	Syslog	NetScreen Firewall events	Yes	Yes	Yes
Juniper Networks	Junos WebApp Secure v4.2.x	Syslog	Incident and access events	Yes	No	No
Juniper Networks	IDP v4.0, v4.1 & v5.0	Syslog	NetScreen IDP events	Yes	No	Yes
Juniper Networks	Network and Security Manager (NSM) and Juniper SSG v2007.1r2 to 2007.2r2, 2008.r1, 2009r1.1, 2010.x	Syslog	NetScreen NSM events	Yes	No	Yes
Juniper Networks	Junos OS v7.x to v10.x Ex Series Ethernet Switch DSM only supports v9.0 to v10.x	Syslog or PCAP Syslog***	All events	Yes**	Yes	Yes
Juniper Networks	Secure Access RA Juniper SA version 6.1R2 and Juniper IC version 2.1	Syslog	All events	Yes	Yes	Yes
Juniper Networks	Juniper Security Binary Log Collector SRX or J Series appliances at v12.1 or above	Binary	Audit, system, firewall, and IPS events	No	No	Yes
Juniper Networks	Steel-Belted Radius v5.x and later	Syslog	All events	Yes	Yes	Yes
Juniper Networks	vGW Virtual Gateway v4.5	Syslog	Firewall, admin, policy and IDS Log events	Yes	No	No
Juniper Networks	Wireless LAN Controller Wireless LAN devices with Mobility System Software (MSS) V7.6 and later	Syslog	All events	Yes	No	No
Kaspersky	Security Center v9.2	JDBC	Antivirus, server, and audit events	No	Yes	No
Lieberman	Random Password Manager v4.8x	Syslog	All events	Yes	No	No
Linux	Open Source Linux OS v2.4 and later	Syslog	Operating system events	Yes	Yes	No
Linux	DHCP Server v2.4 and later	Syslog	All events from a DHCP server	Yes	Yes	No
Linux	IPtables kernel v2.4 and later	Syslog	Accept, Drop, or Reject events	Yes	No	No
McAfee	Intrushield v2.x - v5.x	Syslog	Alert notification events	Yes	No	No
McAfee	Intrushield v6.x - v7.x	Syslog	Alert and fault notification events	Yes	No	No
McAfee	ePolicy Orchestrator v3.5 to v4.6	JDBC, SNMPv2, SNMPv3	AntiVirus events	No	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
McAfee	Application / Change Control v4.5.x	JDBC	Change management events	No	Yes	No
McAfee	Web v6.0.0 and later	Syslog, Log File Protocol	All events	Yes	No	No
MetaInfo	MetaIP v5.7.00-6059 and later	Syslog	All events	Yes	Yes	No
Microsoft	IIS v6.0 and 7.0	Syslog	HTTP status code events	Yes	No	No
Microsoft	Internet and Acceleration (ISA) Server or Threat Management Gateway 2006	Syslog	ISA or TMG events	Yes	No	No
Microsoft	Exchange Server 2007, and 2010	Windows Exchange Protocol	Exchange mail and security events	No	No	No
Microsoft	Endpoint Protection 2012	JDBC	Malware detection events	No	No	No
Microsoft	Hyper V v2008 and v2012	WinCollect	All events	No	No	No
Microsoft	IAS Server v2000, 2003, and 2008	Syslog	All events	Yes	No	No
Microsoft	Microsoft Windows Event Security Log v2000, 2003, 2008, XP, Vista, and Windows 7 (32 or 64-bit systems supported	Syslog or Microsoft Windows Event Log Protocol Source	All events	Yes	Yes	Yes
Microsoft	SQL Server 2008, 2012, and 2014	JDBC	SQL Audit events	No	No	No
Microsoft	SharePoint 2010	JDBC	SharePoint audit, site, and file events	No	No	No
Microsoft	DHCP Server 2000/2003	Syslog	All events	Yes	Yes	No
Microsoft	Operations Manager 2005	JDBC	All events	No	No	No
Microsoft	System Center Operations Manager 2007	JDBC	All events	No	No	No
Motorola	Symbol AP firmware v1.1 to 2.1	Syslog	All events	No	No	No
NetApp	Data ONTAP	Syslog	CIFS events	Yes	Yes	No
Niksun	NetVCR 2005 v3.x	Syslog	Niksun events	No	No	No
Nokia	Firewall NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nokia	VPN-1 NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nominum	Vantio v5.3	Syslog	All events	Yes	No	No
Nortel	Contivity	Syslog	All events	Yes	No	No
Nortel	Application Switch v3.2 and later	Syslog	Status and network condition events	No	Yes	No
Nortel	ARN v15.5	Syslog	All events	Yes	No	No
Nortel	Ethernet Routing Switch 2500 v4.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 4500 v5.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 5500 v5.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8300 v4.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8600 v5.0	Syslog	All events	No	Yes	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Nortel	VPN Gateway v6.0, 7.0.1 and later, v8.x	Syslog	All events	Yes	Yes	No
Nortel	Secure Router v9.3, v10.1	Syslog	All events	Yes	Yes	No
Nortel	Secure Network Access Switch v1.6 and v2.0	Syslog	All events	Yes	Yes	No
Nortel	Switched Firewall 5100 v2.4	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Switched Firewall 6000 v4.2	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Threat Protection System v4.6 and v4.7	Syslog	All events	No	No	No
Novell	eDirectory v2.7	Syslog	All events	Yes	No	No
ObserveIT	ObserveIT 5.6.x and later	Log File Protocol	User activity events	No	No	No
OpenBSD Project	OpenBSD v4.2 and later	Syslog	All events	No	Yes	No
Open LDAP Foundation	Open LDAP 2.4.x	UDP Multiline Syslog	All events	No	No	No
Open Source	SNORT v2.x	Syslog	All events	Yes	No	No
Oracle	Audit Records v9i, v10g, and v11g	Syslog JDBC	All relevant Oracle events	Yes	Yes	No
Oracle	Audit Vault v10.2.3.2 and later	JDBC	Oracle events	No	No	No
Oracle	OS Audit v9i, v10g, and v11g	Syslog	Oracle events	Yes	Yes	No
Oracle	BEA WebLogic v10.3.x	Log File Protocol	Oracle events	No	No	No
Oracle	Database Listener v9i, v10g, and v11g	Syslog	Oracle events	Yes	No	No
Oracle	Fine Grained Auditing v9i and v10g	JDBC	Select, insert, delete, or update events for tables configured with a policy	No	No	No
OSSEC	OSSEC v2.6 and later	Syslog	All relevant	Yes	No	No
Palo Alto Networks	PanOS v3.0 and later	Syslog	All events	Yes	Yes	No
Pirean	Access: One v2.2 with DB2 v9.7	JDBC	Access management and authentication events	No	No	No
PostFix	Mail Transfer Agent v2.6.6 and later	UDP Multiline Protocol or Syslog	Mail events	No	No	No
ProFTPd	ProFTPd v1.2.x, v1.3.x	Syslog	All events	Yes	Yes	No
Proofpoint	Proofpoint Enterprise Protection and Enterprise Privacy versions 7.0.2, 7.1, or 7.2	Syslog	System, email audit, email excryption, and email security threat classification events	No	No	No
Radware	DefensePro v4.23 and 5.01	Syslog	All events	Yes	No	No
Raz-Lee iSecurity	AS/400 iSeries Firewall 15.7 and Audit 11.7	Syslog	Security and audit events	Yes	Yes	No
Redback Networks	ASE v6.1.5	Syslog	All events	Yes	No	No
Riverbed	SteelCentral NetProfiler	JDBC	Alert events	No	No	No
Riverbed	SteelCentral NetProfiler Audit	Log file protocol	Audit events	No	Yes	No
RSA	Authentication Manager v7.1, v6.x	Syslog or Log File Protocol	All events	No	No	No
SafeNet	DataSecure v6.3.0 and later	Syslog	All events	Yes	No	No
Salesforce	Security Auditing	Log File	Setup Audit Records	No	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Salesforce	Security Monitoring	Salesforce REST API Protocol	Login History Account History Case History Entitlement History Service Contract History Contract Line Item History Contract History Contact History Lead History Opportunity History Solution History	No	Yes	No
Samhain Labs	HIDS v2.4	Syslog JDBC	All events	Yes	No	No
Secure Computing	Sidewinder G2 v61	Syslog	All events	Yes	No	No
Sentrigo	Hedgehog v2.5.3	Syslog	All events	Yes	No	No
SolarWinds	Orion v2011.2	Syslog	All events	Yes	No	No
SonicWALL	UTM/Firewall/VPN Appliance v3.x and later	Syslog	All events	Yes	No	No
Sophos	Astaro v8.x	Syslog	All events	Yes	No	No
Sophos	Enterprise Console v4.5.1 and v5.1	Sophos Enterprise Console protocol JDBC	All events	No	No	No
Sophos	PureMessage v3.1.0.0 and later for Microsoft Exchange v5.6.0 for Linux	JDBC	Quarantined email events	No	No	No
Sophos	Web Security Appliance v3.x	Syslog	Transaction log events	Yes	No	No
Sourcefire	Intrusion Sensor IS 500, v2.x, 3.x, 4.x	Syslog	All events	Yes	No	No
Sourcefire	Defense Center v4.8.0.2 and later	Sourcefire Defense Center	All events	No	No	No
Splunk	Microsoft Windows Security Event Log	Windows-based event provided by Splunk Forwarders	All events	No	Yes	No
Squid	Web Proxy v2.5 and later	Syslog	All cache and access log events	Yes	No	No
Startent Networks		Syslog	All events	Yes	No	No
STEALTHbits Technologies	StealthINTERCEPT	Syslog LEEF	Active Directory Audit Events	Yes	No	No
Stonesoft	Management Center v5.4	Syslog	Management Center, IPS, Firewall, and VPN Events	Yes	No	No
Sun	Solaris v5.8, v5.9, Sun OS v5.8, v5.9	Syslog	All events	Yes	Yes	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
Sun	Solaris DHCP v2.8	Syslog	All events	Yes	Yes	No
Sun	Solaris Sendmail v2.x	Syslog	All events	Yes	No	No
Sun	Solaris Basic Security Mode (BSM) v5.10 and later	Log File Protocol	All events	No	Yes	No
Sun	ONE LDAP v11.1	Log File Protocol	All relevant access and LDAP events	No	No	No
Sybase	ASE v15.0 and later	JDBC	All events	No	No	No
Symantec	Endpoint Protection v11 and v12	Syslog	All Audit and Security Logs	Yes	No	Yes
Symantec	SGS Appliance v3.x and later	Syslog	All events	Yes	No	Yes
Symantec	SSC v10.1	JDBC	All events	Yes	No	No
Symantec	Data Loss Prevention (DLP) v8.x and later	Syslog	All events	No	No	No
Symantec	PGP Universal Server 3.0.x	Syslog	All events	Yes	No	No
Symark	PowerBroker 4.0	Syslog	All events	Yes	No	No
ThreatGRID	Malware Threat Intelligence Platform v2.0	Log file protocol Syslog	Malware events	No	No	No
TippingPoint	Intrusion Prevention System (IPS) v1.4.2 to v3.2.x	Syslog	All events	No	No	No
TippingPoint	X505/X506 v2.5 and later	Syslog	All events	Yes	Yes	No
Top Layer	IPS 5500 v4.1 and later	Syslog	All events	Yes	No	No
Trend Micro	Control Manager v5.0 or v5.5 with hotfix 1697 or hotfix 1713 after SP1 Patch 1	SNMPv1 SNMPv2 SNMPv3	All events	Yes	No	No
Trend Micro	Deep Discovery v3.x	Syslog	All events	Yes	No	No
Trend Micro	InterScan VirusWall v6.0 and later	Syslog	All events	Yes	No	No
Trend Micro	Office Scan v8.x and v10.x	SNMPv2	All events	No	No	No
Tripwire	Enterprise Manager v5.2 and later	Syslog	Resource additions, removal, and modification events	Yes	No	No
Tropos Networks	Tropos Control v7.7	Syslog	Fault management, login/logout, provision, and device image upload events	No	No	No
Trusteer	Apex Local Event Aggregator v1304.x and later	Syslog	Malware, exploit, and data exfiltration detection events	Yes	No	No
Universal	Syslog and SNMP	Syslog SNMP SDEE	All events	No	Yes	No
Universal	Syslog	Syslog Log File Protocol	All events	No	Yes	No
Universal	Authentication Server	Syslog	All events	No	Yes	No
Universal	Firewall	Syslog	All events	No	No	No
Verdasys	Digital Guardian 6.0.x	Syslog	All events	Yes	No	No
Vericept	Content 360 up to v8.0	Syslog	All events	Yes	No	No

Table 1. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded Events	Auto discovered?	Includes identity?	Includes custom properties?
VMware	VMware ESX or ESXi 3.5.x, 4.x, and 5.x	Syslog VMWare protocol	All events	Yes if syslog	No	No
VMware	vCenter v5.x	VMWare protocol	All events	No	No	No
VMware	vCloud v5.1	vCloud protocol	All events	No	Yes	No
VMWare	vShield	Syslog	All events	Yes	No	No
Vormetric, Inc.	Vormetric Data Security	Syslog (LEEF)	Audit Alarm Warn Learn Mode System	Yes	No	No
Websense	TRITON v7.7	Syslog	All events	Yes	No	No
Websense	V Series Data Security Suite (DSS) v7.1.x and later	Syslog	All events	Yes	No	No
Websense	V Series Content Gateway v7.1.x and later	Log File Protocol	All events	No	No	No
Zscaler	Zscaler NSS v4.1	Syslog	Web log events	Yes	No	No