RSA enVision
Supported Event Sources

Created on Wednesday, June 19, 2013.

Table of Contents

RSA Supported Event Sources

The following is an alphabetical list of supported event sources sorted by partner name that are available in the monthly Content Event Source Updates (ESUs). Contact RSA Customer Support for the latest status and details of the integration. If you are unable to find your event source from our list of supported event sources, visit http://www.rsa.com/go/partners/suggest_new.asp.

A B C D E F G H I J K L M N O P Q R S T V W Z

A

Vendor	Device	Collection Method
Actiance	Actiance Vantage - **version 12.2**	ODBC
Actividentity	4TRESS AAA Server - **version 6.4.1**	ODBC
Airmagnet	AirMagnet Enterprise - **version 7.5.0, 8.5, 10.1**	Syslog
Alcatel-Lucent	OmniSwitch - **versions 6850 & 9700**	Syslog, SNMP
Apache	HTTP Server - **versions 2.1, 2.2, 2.4**	File Reader
Apache	Tomcat Server - **version 6.0 and 7.0**	File Reader
Apple	Mac OS X - **version 10.4.3 Build 8F46**	Syslog
Application Security	DbProtect - **version 6.0**	ODBC
Arbor Networks	Peakflow SP5 - **version 5.0**	Syslog
Arbor Networks	Peakflow X - **version 4.1**	Syslog
Aruba Networks	Aruba Networks AirWave - **version 7.5.1**	Syslog
Aruba Networks	Aruba Networks ClearPass Policy Manager- **version 5.2**	Syslog
Aruba Networks	Aruba Networks Mobility Controller - **version ArubaOS 2.5.4.0, 3.4, 6.1.2.2**	Syslog
Astaro	Security Gateway - **version 7.x**	Syslog
Avecto	Privilege Guard - **version 3.5**	Windows event logs
Avocent	Avocent IP KVM - **version Dell PowerEdge 2161DS-2**	SNMP - parser trap handler

B

Vendor	Device	Collection Method
Barracuda Networks	Spam Firewall - **version 3.4 & 3.5**	Syslog
Barracuda Networks	Web Application Firewall - **firmware version 7.4.0**	Syslog
Bee Ware	Web Application Firewall - **version 5.3.1**	Syslog
BigFix	BigFix Enterprise Suite - **version 7.2**	ODBC
Bit9	Bit9 Parity - **version 6.0.2**	Syslog, ODBC
Blue Coat Systems	CacheOS (CacheFlow Appliance) - **versions 4.1, 4.2, 5.1, 5.2, 5.3, 5.4, 5.4.1.12**	File Reader
Blue Coat Systems	Director - **version 5.5.1.1, 5.5.2.3, 6.1.1.1**	Syslog
Blue Coat Systems	ProxyAV - **version 3.3.1.2**	Syslog and SNMP
Blue Coat Systems	ProxySG SGOS (Security Gateway Appliance) - **versions 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 5.4, 5.4.2, 5.4.3.2, 5.4.3.7, 5.4.6.1, 5.5.1.1, 5.5.5.1, 6.1.1.1, 6.1.3.1, 6.1.4.1, and 6.3.5.1**	File Reader
BMC	Remedy IT Service Management - **versions 7.6.04**	ODBC
Brocade	FastIron Switch - **version FGS624P- STK**	Syslog

C

Vendor	Device	Collection Method
CA	ACF2 z/OS - **version r14, r15**	File Reader
CA	Integrated Threat Management - **version r8, 8.1**	SNMP
CA	SiteMinder - **version r12**	File Reader
CA	Top Secret - **version 1.4**	File Reader
CentOS	CentOS -**version 6.0**	Syslog
Check Point	Check Point Security Suite, IPS-1- **versions R54 - R65, R70, R71, R75, R75.40 GAIA OS**	OPSEC LEA
Check Point	IPSO - **version 3.5 and earlier, 3.6, 3.7, 3.8, 3.9, 6.2**	Syslog and SNMP
Check Point	SPLAT OS - **R75**	Syslog
Cisco	Access Control Server - **versions 3.3, 4.0, 4.2 (software only)** Access Control Server - **versions 4.0, 4.1, 4.2, 5.1, 5.2(appliance)**	File Reader and Syslog
Cisco	Adaptive Security Appliance Software - **versions 7.1(2), 7.2, 8.0, 8.2, 8.4 (to generate syslog events)** ASA Security Services Module Software - **version 5.1(1p1) (to generate IDS events)**	Syslog
Cisco	Aggregation Services Router **version 3.3**	Syslog
Cisco	Aironet AP (Wireless Access Point) - **version IOS 12.2**	Syslog
Cisco	Application Control Engine - **version 4710**	Syslog
Cisco	Catalyst Switch 6500 CATOS , Cisco IOS 12.4 - **version 8.3 (alerting only)**	Syslog
Cisco	CiscoWorks Network Compliance Manager - **version 1.4 SP2**	ODBC
Cisco	Content Engine - **versions 5.0, 5.4, 5.5**	File Reader and Syslog
Cisco	Content Services Switch - **versions 5.10, 8.10**	Syslog
Cisco	Firewall Service Module - **version 4.1(5)**	Syslog
Cisco	Identity Services Engine **version 1.0, 1.1**	Syslog
Cisco	IronPort Email Security Appliance - **versions 5.7.0, 7.1.3**	File Reader
Cisco	IronPort Web Security Appliance - **version 5.7.0, 6.3, 7.1.1, 7.1.3, and 7.5**	File Reader and Syslog
Cisco	LAN Management Solution - **version 3.2 and 4.0**	ODBC

Vendor	Device	Collection Method
Cisco	Monitoring, Analysis, and Response System (MARS) - **version 6.0.3, 6.0.7, 6.0.8, 6.1**.	File Reader and Syslog
Cisco	Mobility Services Engine - **versions 5.2.91.0, 6.0.97.0, 7.0.105.0**	Syslog
Cisco	Multilayer Director Switch - **version 3.3 (4A)**	Syslog
Cisco	Network Admission Control - **version 4.7, 4.9**	Syslog
Cisco	Nexus - **version 1000V, 5000V, and 7000V**	Syslog
Cisco	PIX Firewall - **version 7.0, 8.0**	Syslog
Cisco	Prime Infrastructure - **version 1.1, 1.2**	SNMP
Cisco	Router - **version IOS 12.4, 15**	Syslog
Cisco	Secure Access Control Server - **versions 4.0, 4.1, 4.2, 5.1, 5.2, 5.3**	File Reader and Syslog
Cisco	Secure Access Control Server Express - **version 5.0**	Syslog
Cisco	Secure IDS/IPS - **versions 4.x, 5.0, 5.1, 6.0, 6.1, 6.2, 7.0, 7.1.1**	SDEE, RDEP (prior to RSA enVision 4.0)
Cisco	Security Agent - **versions 4.0, 5.1, 6.0**	SNMP and ODBC
Cisco	Security Manager (also branded as CiscoWorks Common Services) - **version 2.3, 3.0, 3.3, 4.0**	File Reader
Cisco	Unified Computing System Manager - **version 1.0 (2d)**	Syslog
Cisco	Virtual Security Gateway version 4.2(1)VSG(1)	Syslog
Cisco	VPN 3000 Concentrator - **versions 3.6.7 , 4.0, 4.1, 4.7**	Syslog
Cisco	Wireless Control System - **version 7.0**	SNMP
Cisco	Wireless LAN Controller (WLC) - **versions 5.2.157.0, 6.0.188, 7.0.98.0**	Syslog and SNMP
Citrix	Access Gateway - **version 4.5 and 4.6**	Syslog
Citrix	NetScaler - **versions 9.1, 9.2, 9.3**	Syslog
Citrix	XenApp - **5 (for Windows Server 2003) and 6**	ODBC
Courion	PasswordCourier - **version 5.0**	File Reader
Crossbeam Systems	C-Series - **versions 4.X, 5.X, 6.X**	Syslog
Cyber-Ark	Enterprise Password Vault, Inter-Business Vault, and Sensitive Document Vault - **version 5.0**	Syslog
CyberGuard	Firewall TSP Family Series - **version 6.4.1**	Syslog
CyberGuard	Cyberguard Classic - **version 5.2 P4**	Syslog

D

Vendor	Device	Collection Method
Damballa	Damballa Failsafe - **version 4.0.2**	Syslog
Debian	Debian GNU/Linux - **versions 3.1 and 4.0**	Syslog
Dell	iDRAC (Integrated Dell Remote Access Controller) -**version 5.0, 6.0**	SNMP
Dell	PowerConnect 5324 Switch - **version 1.0.0.47**	Syslog

E

Vendor	Device	Collection Method
eEye	Blink Endpoint Protection - **version 4.6**	SNMP
eEye	REM Security Management Console - **version 3.7**	SNMP
eEye	Retina Network Security Scanner - **version 5.10**	Syslog and SNMP

Vendor	Device	Collection Method
EMC	Avamar - **version 4.1 and 6.0**	ODBC
EMC	Celerra - **version 5.5, 5.6, and 6.0** (branded as: EMC Control Station, Blades, DataMover)	SNMP and NIC Windows Service
EMC	Clariion / VNX - **version Navisphere 6.28 and Unisphere 1.1**	SNMP
EMC	Data Domain - **version 5.1.0.4**	Syslog
EMC	Data Protection Advisor - **version 5.6**	ODBC
EMC	Documentum - **version 6.5 and 6.7**	ODBC
EMC	Fabric OS - **version 6.1, 6.2**	Syslog
EMC	Greenplum Database - **version 4.0**	File Reader
EMC	Greenplum HD - **version 1.2**	File Reader
EMC	Ionix SCM (Server Configuration Manager) - **version 5.2**	Windows Event Logs
EMC	Ionix Unified Infrastructure Manager (UIM) - **version 1.0, 2.1, 3.0, and 3.1**	ODBC, Syslog, File Reader (3.1. Patch 1 only)
EMC	Isilon - **version 6.5.3.32, 6.5.5.7**	File Reader
EMC	NetWorker **version 7.6 SP2**	File Reader
EMC	Secure Remote Support - **version 2.0**	Syslog
EMC	Symmetrix Solutions Enabler - **version 6.4, 6.5.3, 7.0, 7.1, and 7.3.0.1** Symmetrix V-Max	Syslog and NIC Windows Service
EMC	Voyence - **version 4.0.1**	SNMP
EMC	VPLEX	File Reader
Enterprise IT-Security	SF-NoEvasion - **version 7.1**	Syslog
Enterasys Networks	Dragon - **version 5.x, 6.x, 7.2, 7.4**	SNMP
Enterasys Networks	Switch - **N-Series and S-Series**	Syslog
Extreme Networks	ExtremeWare Switch - **version 6.2, 7.2, 7.7**	Syslog
Extreme Networks	ExtremeXOS - **version 12.2.1.1**	Syslog

F

Vendor	Device	Collection Method
F-Secure	F-Secure Anti-Virus for Windows Servers, F-Secure Client Security, F-Secure Linux Security	Syslog and Windows event logs
F5	BigIP Local Traffic Manager - **version 9.4, 10.2.0, 11.1, 11.2.1**	Syslog
F5	BigIP Access Policy Manager - **version 10.2.0**	Syslog
F5	BigIP Application Security Manager **version 10.2.0, 11.2**	Syslog
F5	F5 Firepass - **version 5.5-20051019, 7.0.1**	Syslog
FairWarning	Privacy Monitoring **version 2.9.2**	SFTP
FireEye	Web Malware Protection System **version 6.x**	Syslog
ForeScout	CounterACT **version 6.3.4.0**	Syslog
Fortinet	FortiGate Antivirus Firewall, running FortiOS - **version 2.8, 3.0, 4.0 MR1, 4.0 MR2**	Syslog
Fortinet	FotiClient Endpoint Security - **version 4.2.3.271**	Syslog
Fortinet	FortiMail - **version 4.0**	Syslog
Foundry Networks	Switch - **version 07**	Syslog
FreeBSD	FreeBSD - **version 5.4**	Syslog

G

Vendor	Device	Collection Method
GE Healthcare	GE Centricity PACS-IW - **version 3.7.3**	ODBC
GE Healthcare	GE Centricity Enterprise Archive- **version 4.0**	ODBC
GIT	GIT **version 1.7.6**	File Reader
GlobalScape	EFT Server **all versions up to 6.3.8**	File Reader

H

Vendor	Device	Collection Method
HP	Integrity NonStop Server - **5.3**	Syslog
HP	Open VMS - **all versions**	File Reader
HP	ProCurve Switch series 2600, 2800, 5300	Syslog
HP	HP TippingPoint Security Management System (SMS) - **versions 2.1, 2.5, 2.6, 2.7, 3.0, 3.1, 3.2, 3.5**	Syslog
HP	UX - **version 11.X, C2 v11.X**	Syslog
Huawei	VRP - **version 5.20, 5.30**	Syslog
HyTrust	HyTrust Appliance - **version 2.0.10264, 2.5.1, and 3.0.2**	Syslog

I

Vendor	Device	Collection Method
IBM	AIX 5L (Security and Authentication messages only), 6.1, 7.1	Syslog and Syslog NG
IBM	iSeries AS400 - **V5R2 and later**	File Reader
IBM (Lotus)	Lotus Domino - **versions 7, 8, 8.5**	SNMP
IBM	DB2 UDB - **versions 7, 8, 8.1, 9.1, 9.5, 9.7**	File Reader
IBM	Guardium SQL Guard - **versions 7, 8.0.2, and 9**	Syslog
IBM	Mainframe ICSF - **all versions**	File Reader
IBM	Mainframe IDMS - **all versions**	File Reader
IBM	Mainframe IMS - **all versions**	File Reader
IBM	Mainframe IPSec - **all versions**	File Reader
IBM	Mainframe SMA_RT OS390/ZOS - **version 2.0.6**	Syslog
IBM	Mainframe RACF ZOS - **all versions**	File Reader
IBM	Mainframe Syslog and Hardcopy Log Facility - **version 2.0.6**	File Reader
IBM	ISS Product suite: Proventia Appliance, SiteProtector, Internet Scanner, RealSecure - **Site Protector v2.0 SP6.1, SP7.0, SP8.0, SP8.1, and SP9.0**	ODBC
IBM	Tivoli Access Manager for Enterprise Single Sign-On - **version 8.0.1**	ODBC
IBM	Tivoli Access Manager WebSEAL - **version 6.0**	File Reader
IBM	Tivoli Identity Manager - **version 5.1**	ODBC
IBM	Websphere - **version 6.0.0.1/Microsoft Windows 2003, version 8.0/Microsft Windows 2008 R2** Websphere**version 7.0.0.9/Redhat Linux/Solaris/IBM AIX 6.0**	File Reader
IBM	Websphere DataPower- **version 3.8.1**	Syslog

Vendor	Device	Collection Method
IBM	Websphere MQ- **version 7.0.1**	File Reader
Imperva	SecureSphere - **versions 6, 7, 8, 8.5, 9**	Syslog
Infoblox	NIOS - **version 5.1 and 6.4.5 for Linux**	Syslog
Intel	NetStructure VPN - **version 6.9**	Syslog
Intersect Alliance	Snare for Linux - **version 1.5.1**	Syslog
Invincea	Invincea Threat Data Server - **version 2.6**	Syslog
Ipswitch	WhatsUp Gold - **version 14.2**	ODBC

J

Vendor	Device	Collection Method
J4Care	Healthcare Connector	Syslog
JBoss	JBoss Application Server - **versions 4.1 and 5.0**	File Reader
Juniper Networks	DX Application Accelerator - **version 5.1.5**	Syslog
Juniper Networks	IDP - **versions 3.0, 3.1, 3.2, 4.0, 4.1, 5.0**	Syslog and File Reader
Juniper Networks	JUNOS Router - **version 6.1, JUNOS 9.4, 9.6, 10.0, 10.3, 11.1, 11.2, 11.4, 12.1**, SRX Series	Syslog
Juniper Networks	NetScreen Firewall Screen OS - **versions 5.1, 5.3, 5.4, 6.0**	Syslog
Juniper Networks	NetScreen ScreenOS **versions 5.1, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3**	Syslog
Juniper Networks	NetScreen-Security Manager - **versions 2004, 2006, 2007, 2010, and 2011**	Syslog and File Reader
Juniper Networks	SSL VPN - **versions 5.4, 5.5, 6.0, 6.2 R2, 6.5 R2, 7.0 R2, 7.1 R5, 7.2 R1**	Syslog
Juniper Networks	Steel-Belted Radius - **version 5.4 and 6.1.6**	File Reader
Juniper Networks	Unified Access Control - **version 2.2, 3.1, and 4.5**	Syslog
Juniper Networks	Wireless LAN Controller - **version 7.6.1**	Syslog

K

Vendor	Device	Collection Method
Kasperksy	Administration Kit 8.0 Security Center 9.0 Anti-Virus for Microsoft ISA 2004 and 2008.	ODBC

L

Vendor	Device	Collection Method
Lancope	StealthWatch - **versions 5.5, 5.6, 5.9, 5.10, 6.0** (StealthWatch Xe for NetFlow, StealthWatch Xe for sFlow, StealthWatch NC)	Syslog
LANDesk	Management Suite - **version 9.0 Service Pack 2**	ODBC
Lumension	Endpoint Management and Security Suite - **version 7.0**	ODBC

M

Vendor	Device	Collection Method
ManageEngine	Netflow Analyzer - **version 8.0 and 9.5**	ODBC
Mazu Networks	Mazu Profiler - **versions 5.5.2, 6.0, 7.0**	SNMP
McAfee	Database Security - **version 4.2**	Syslog

Vendor	Device	Collection Method
McAfee	Email Gateway - **version 5.5, 7.0**	SNMP and Syslog
McAfee	Endpoint Encryption - **version 5.2.2 and 5.2.12**	SFTP and File Reader
McAfee	ePolicy Orchestrator - **versions 3.5, 3.6.0, 3.6.1, 4.0, 4.5, and 4.6** **Note**: RSA enVision 3.7 and later is required for version 4.0, 4.5, and 4.6.	ODBC
McAfee	Firewall Enterprise - **versions 6.1.1.x, 6.1.2.x, 7.0.0.x, 8.0, 8.2**	Syslog
McAfee	Host Data Loss Prevention - **versions 2.2, 3.0, 9.0, 9.1, and 9.2**	ODBC
McAfee	Host Intrusion Prevention (also branded as Entercept): • **version 6.0.1** supported on McAfee ePolicy Orchestrator version 3.6 • **version 7.0 and 8.0** supported on McAfee ePolicy Orchestrator version 4.0	ODBC
McAfee	Integrity Control **versions 5.0.2, 5.1.0, and 6.0.1**	ODBC
McAfee	McAfee Network Security Platform (formerly IntruShield)- **versions 2.1, 3.1, 4.1, 5.1, 6.1, 7.1**	Syslog and ODBC (for version 5.1)
McAfee	Network Access Control - **version 3.1.1**	ODBC
McAfee	Network Data Loss Prevention - **version 8.6**	ODBC
McAfee	Policy Auditor - **version 5.2 and 6.01**	ODBC
McAfee	VirusScan Enterprise - **version 8.0i, 8.5i, 8.7i, and 8.8**	ODBC and Windows Event Logs
McAfee	Vulnerability Manager (formerly known as Foundscan Professional/Enterprise) - **versions 5.0, 6.5.1, 6.8, 7.0**	ODBC
McAfee	Web Gateway - **version 6.8.5, 7.0, 7.1, 7.2**	File Reader
McKesson	Horizon Patient Folder - **version 15**	ODBC
Microdasys	XML Security Gateway - **version 1.1.0**	File Reader
Microsoft	Audit Collection Service - **version 2007 SP1**	ODBC
Microsoft	DHCP Server for **Windows 2000, 2003, 2008, 2012**	File Reader
Microsoft	Endpoint Protection 2010	ODBC and Windows Event Logs
Microsoft	Exchange Server - **versions 2003, 2007, and 2010**	File Reader and Windows Event Logs
Microsoft	Forefront Client Security **version 1.1 and 1.5**	ODBC
Microsoft	Forefront Threat Management Gateway - **version Beta, ISA 2006, TMG 2010**	File Reader, SFTP Agent, and ODBC
Microsoft	Forefront Unified Access Gateway - **version 2010**	Syslog and ODBC
Microsoft	Internet Information Services (IIS) - **versions 5.x, 6.x, 7.x**	File Reader
Microsoft	Internet Security and Acceleration (ISA) Server - **versions 2000, 2004, 2006**	File Reader and Windows Event Logs
Microsoft	Network Access Protection - **version 1.1**	ODBC
Microsoft	Network Policy Server (formerly Internet Authentication Service) **version 2003, 2008**	File Reader and Windows Event Logs
Microsoft	SharePoint Server - **versions 2007 and 2010**	Agentless Windows
Microsoft	System Center Operations Manager - **version 2005, 2007, and 2012**	Agentless Windows
Microsoft	System Center Configuration Manager - **versions 2007 and 2012**	Agentless Windows
Microsoft	SQL Server - **version 2000, 2005, 2008, and 2012**	ODBC, File Reader,, and Windows Event Logs
Microsoft	Windows (agentless)	Windows Event Logs

Vendor	Device	Collection Method
Microsoft	Windows (via third party collection agent) - Adiscon Event Reporter & DNS Server	Syslog via Agent
Microsoft	Windows (via third party collection agent) - InterSect-Alliance BackLog	Syslog via Agent
Microsoft	Windows (via third party collection agent) - InterSect Alliance SNARE	Syslog via Agent
Microsoft	Windows Server Update Service - **version 3.0 SP 2**	ODBC
Motorola	AirDefense Enterprise Server - **version 7.2, 7.3**	Syslog
MySQL	MySQL Enterprise - **version 5.1**	SNMP

N

Vendor	Device	Collection Method
nCircle	Configuration Compliance Manager **version 5.10**	Syslog
nCircle	nCircle IP360 - **versions 5.5, 6.5, 6.8**	XML3
NETASQ	Unified Manager - **version 8.1.3 and 9.0.2**	Syslog
NetContinuum	NetContinuum Web Application Firewall - **version NC OS 5.x**	Syslog
Network Appliance	Data ONTAP - **version 6.x through 8.0.2**	Syslog
Network Appliance	NetCache - **version 5.5R3, 5.6.2R1, 6.03, 6.1**	File Reader
NFR	NIDS - **version 3.x, 4.x, 5.x**	Syslog
Nortel	Alteon Switch Firewall - **version 8.x**	Syslog
Nortel	Contivity VPN Switch	Syslog
Nortel	Passport 8600 Routing Switch - **version 3.7.5.2** (rebranded to Ethernet Routing Switch 8600)	Syslog
Novell	eDirectory - **version 8.8** for Windows and Linux	SNMP
Novell	SuSE Linux - **version 9, 10, 10.2, and 11**	Syslog

O

Vendor	Device	Collection Method
Open Source	KVM- **versions 2.6.32-220**	File Reader
Open Source	NFDump - **netflow v5, v7, v9 / NFDump v1.5.7**	File Reader
Open Source	SNORT - **version 2.8 (signature level 1.41.2.14), and 2.9**	Syslog
Open Source	Squid - **versions 2.5.9, 2.7, 3.0, 3.1.05, and 3.1.20**	File Reader
Oracle	Audit Vault - **version 10.3**	ODBC
Oracle	Database - **versions 8i, 9i, 10g, 11g, and 11.2g**	ODBC, File Reader, Syslog, and Windows Event Logs, XML
Oracle	Internet Directory - **version 10.1**	ODBC
Oracle	Identity Manager - **version 9.1**	ODBC
Oracle	iPlanet Web Server **version 6.1 and 7**	File Reader and SFTP
Oracle	Database Vault - **version 10g R2**	ODBC
Oracle	Oracle WebLogic - **version 10.0, 10.3, 10.3.2, and 10.3.5**	File Reader

P

Vendor	Device	Collection Method
Palo Alto	Networks Firewall - **versions PA-200, PA-500, PA-2000 Series, PA-4000 Series, and PA-5000 Series**	Syslog
Palo Alto	Panorama Management Server - **version 4.1**	Syslog
Perforce	Perforce	File Reader
PosgreSQL	PosgreSQL - **version 8.4**	Syslog
Proofpoint	Email Security- **version 6.3**	Syslog

Q

Vendor	Device	Collection Method
Qualys	QualysGuard- **versions 6.5, and 6.6**	HTTPS

R

Vendor	Device	Collection Method
Radware	Radware DefensePro - **version 5.01.02, 6.05**	Syslog and SNMP
Rapid7	NeXpose - **versions 4.8, 5.0**	File Reader
Research in Motion	BlackBerry Enterprise Server - **version 5.0**	File Reader
Red Hat	Red Hat Enterprise Linux - **versions 3.x, 4.x, 5.x, and 6.0**	Syslog
Riverbed	Riverbed Cascade Express - **version 9.5.1**	SNMP
Riverbed	Riverbed Steelhead - **version 7.0.2**	SNMP and Syslog
RSA Security	Access Manager - **version 6.0, 6.2 on Solaris, Windows, and Linux**	File Reader
RSA Security	Adaptive Authentication (Hosted) - **versions 8.8, 8.9, 9.0, 9.1**	SFTP Agent and File Reader
RSA Security	Adaptive Authentication (OnPrem) - **version 6.0.2.1**	Syslog
RSA Security	Archer - **version 5.1**	ODBC
RSA Security	Authentication Manager Express **1.0**	Syslog and File Reader
RSA Security	Authentication Manager and User Credential Manager - **versions 5.2, 6.0, 6.1, 7.1 SP2, 7.1 SP4, and 8.0**	File Reader Syslog for RSA Authentication Manager 7.1 and later
RSA Security	Certificate Manager - **version 6.8**	SFTP and File Reader
RSA Security	Data Loss Prevention - **version 7.0.0, 8.0, 8.0 SP1, 8.5 8.8, 9.0, and 9.5**	Syslog
RSA Security	Data Protection Manager (formerly Key Manager) - **version 2.1.3, 2.5, 2.7, 3.1**	Syslog
RSA Security	Federated Identity Manger - **version 4.1**	File Reader
RSA Security	NetWitness Informer- **version 2**	Syslog and Windows Event Logs
RSA Security	NetWitness NextGen - **version 9**	Syslog
RSA Security	NetWitness Spectrum - **version 1.0.5.0**	Syslog
RSA Security	Virtual Log Router - **version 1.1**	Syslog

S

Vendor	Device	Collection Method
Safend	Protector - **version 3.3**	Syslog
Safestone	DetectIT **version 14.3**	Syslog
SAP	SAP ERP Central Component - **version 4.6 through 7.2**	File Reader

Vendor	Device	Collection Method
SECUDE	Security Intelligence - **version 1.0**	File Reader
Silver Peak	WAN - **version 5.1.1.0**	Syslog
Silver Tail Systems	Forensics and Mitigator - **version 1.x, 2.x, and 3.x**	Syslog
Solsoft	NP - **version 5.2.4**	Syslog
SonicWALL	E-Class SRA / Aventail SSL VPN - **version 8.8, 9.0, 10.0**	File Reader and Syslog
SonicWALL	Email Security - **version 7.2**	Syslog
SonicWALL	Firewall (alerting only)	Syslog
SonicWALL	Global Management System - **version 6.0**	ODBC
Sophos	Endpoint Security, Enterprise Console - **version 3.0, 4.5, 4.7**	SNMP and ODBC
Sourcefire	Sourcefire Defense Center - **version 4.6, 4.8. 4.9, 4.10, and 5.1**	Syslog
Sun	Solaris - **versions 2.8, 2.9, 2.10**	Syslog
Sun	Solaris Basic Security Module (BSM) - **versions 8, 9, 10, 11**	File Reader and Syslog
Sun	Sun ONE Directory Server - **version 5.2**	File Reader
Sybase	Sybase Adaptive Server Enterprise - **version 15**	ODBC
Symantec	Brightmail - **version 9.5.3**	Syslog
Symantec	Critical Systems Protection - **versions 5.2.4, 5.2.8, 5.2.9**	ODBC
Symantec	Data Loss Prevention - **version 10.5.1**	Syslog
Symantec	Endpoint Protection - **versions 9.0, 10.0, 10.1, 10.2, 11, 11.0.5, 11.0.6, 12, and 12.1**	SNMP, Syslog, and ODBC
Symantec	Enterprise Firewall - **versions 6.x, 7.x, 8.x**	SNMP
Symantec	Intruder Alert - **version 3.6**	SNMP
Symantec	Network Security - **version 4.0**	Syslog

T

Vendor	Device	Collection Method
Tenable	Nessus - **versions 5.0, 4.4, 4.2, 4.0.1, 3.0.6, 1.0.2**	File Reader
Teradata	Database - **version 14.0**	ODBC
Top Layer	Attack Mitigator - **version 2.1**	Syslog
Top Layer	Secure Edge Controller - **version 2.01**	Syslog
Trend Micro	Deep Security - **version 7.0, 7.5 and 8.0**	Syslog
Trend Micro	Deep Security Agent - **version 7.0 and 7.5**	Syslog
Trend Micro	InterScan Messaging Security Suite - **version 7.1**	SNMP and File Reader
Trend Micro	InterScan Web Security - **version 3.1 and 5.6**	ODBC and File Reader
Trend Micro	OfficeScan Corporate Edition - **version 7.0, 8.0, 10.0, 10.5, and 10.6** Control Manager **- version 3.5, 5.0, 5.5**	SNMP and Syslog
Trend Micro	OSSEC **version 2.5.1, 2.6**	Syslog
Trend Micro	ScanMail - **ScanMail 8.0 Service Pack 1 for Microsoft Exchange 2000, 2003, 2007, ScanMail 10.2**	SNMP
Trend Micro	Server Protect - **version 5.8**	SNMP
Tripwire	Tripwire Enterprise - **versions 5.4, 5.5, 7.5, 8.0**	File Reader and Syslog (for version 8.0)
Tufin	Tufin SecureTrack - **version 12.2**	Syslog

V

Vendor	Device	Collection Method
Varonis	DatAdvantage - **version 5.5**	ODBC
VMware	vCloud Director- **version 1.0**	Syslog
VMware	VMware VirtualCenter server- **versions 2.0.2 and 2.5** VMware vCenter Server **versions 4.1, 5.0, and 5.1** VMware ESX - **versions 3.0.3, 3.5, 4.0, 4.1** VMware ESXi - **versions 3.5, 4.0, 4.1, 5.0, and 5.1** VMware Embedded ESXi - **versions 3.5 and 4.0**	Syslog
VMware	vShield **versions 4.1 and 5.0**	Syslog
VMware	VMware View - **versions 3.1, 4.0, 4.5, 4.6, 5.0, and 5.1**	SFTP , File Reader, and ODBC
Voltage	SecureData - **version 5.0 and 5.5**	Syslog
VSS Monitoring	VSS Monitoring - **version 2.3**	SNMP

W

Vendor	Device	Collection Method
WebSense	Web Security - **versions 5.5, 6.3, 7.0, 7.1, 7.5, 7.6, and 7.7**	SNMP, Syslog, and ODBC

Z

Vendor	Device	Collection Method
Zenprise	MobileManager - **version 6.6**	Syslog

Partner Created Event Sources

The following is an alphabetical list of partner created device support in collaboration with the RSA Secured® Technology Partner Program. The RSA Secured Technology Partner Program for RSA enVision combines the best-in-class partner framework of RSA's Technology Partner Program with the RSA enVision EventSource Integrator (ESI) tool to allow device manufacturers the ability to create their own event support. The partner created content will be subject to review and certification by RSA. On successful certification, the content will be available for download from the RSA enVision Intelligence Community at https://rsaenvision.lithium.com/.

A B C E F H J L M N O P R S

A

Vendor	Device	Collection Method
AirTight Networks	SpectraGuard Enterprise - **versions 6.5, 6.6, and 6.7**	Syslog
Array Networks	SPX Series Universal Access Controllers - **version 8.4.6**	Syslog

B

Vendor	Device	Collection Method
BeyondTrust Software	PowerBroker - **version 7**	Syslog

C

Vendor	Device	Collection Method
Cimcor	CimTrak - **version 2.0.6.11**	Syslog
CoreTrace	Bouncer - **version 6.0.1**	Syslog
CounterTack	Event Horizon - **version 3.1**	Syslog

E

Vendor	Device	Collection Method
ESET	Remote Administrator - **versions 4.0 and 5.0**	ODBC
Enforcive	Enterprise Security - **version 7.2.1**	Syslog

F

Vendor	Device	Collection Method
FireEye	Malware Protection System (MPS) - **versions 5.1, 5.2, and 6.2**	Syslog
FoxT	Server Control - **version 6.5 and 6.6**	Syslog

H

Vendor	Device	Collection Method
Help Systems	PowerTech Interact - **version 4.1**	Syslog
Hitachi ID Systems	Privileged Access Manager - **versions 7.1.X, 7.2.X, 7.3.x**	ODBC
Hitachi ID Systems	Password Manager - **versions 7.1.X, 7.2.X, 7.3.x**	ODBC

J

Vendor	Device	Collection Method
Juniper Networks	Altor Networks Security Suite - **version 4.0**	Syslog

L

Vendor	Device	Collection Method
Lieberman Software	Enterprise Random Password Manager - **version 4.83.1**	Syslog

M

Vendor	Device	Collection Method
M86 Security	Secure Web Gateway - **version 10.1 and 10.2**	Syslog

N

Vendor	Device	Collection Method
NetClarity	NACwall - **version 8.0.6**	Syslog
Nominum	Vantio - **version 5.2**	Syslog

O

Vendor	Device	Collection Method
ObserveIT	ObserveIT - **version 5.5**	ODBC

P

Vendor	Device	Collection Method
PowerTech	Interact for IBM iSeries - **version 3**	Syslog

R

Vendor	Device	Collection Method
Raz-Lee	iSecurity for IBM iSeries - **version 11.4**	Syslog

S

Vendor	Device	Collection Method
Stonesoft	StoneGate Management Center - **version 5.3**	Syslog