The HP ArcSight library of out of the box SmartConnectors provides source-optimized collection for 310+ commercial products. These products span the entire stack of event-generating source types, from network and security devices to databases and enterprise applications. SmartConnectors are the default listing in this document.

In addition to SmartConnectors developed and maintained by HP ArcSight, we test and certify the following connector types through our Technology Alliances Program:

- CEF Certified: Ensures event information is captured properly in the (Common Event Format)
- Action Certified: Allows for control of a vendor’s technology from within the ArcSight console.

### Anti-Virus/Anti-Spam
- F-Secure Anti Virus
- Kaspersky Anti-Virus
- McAfee VirusScan Enterprise
- Sophos
- Sybari Antigen for Microsoft Exchange
- Symantec Endpoint Protection Manager (SEPM) database SEP 12
- Symantec Mail Security for MS Exchange
- TrendMicro OfficeScan (Control Manager, TM Control Manager DB)
- TrendMicro VirusWall (Control Manager)

### Applications
- IBM WebSphere
- Oracle Weblogic Server (BEA)
- SAP ERP

### Application Security
- Arxan GuardIT – (CEF)
- Bit9 Parity Suite – (CEF)
- Layer7 SecureSpan/CloudSpan Gateway – (CEF)
- McAfee Application Control (SolidCore)
- Silver Tail Systems Forensics – (CEF)

### Clinical / Healthcare Applications
- FairWarning – (CEF)

### Content Security
- Aladdin eSafe Gateway
- Barracuda (NetContinuum Web Firewall)
- McAfee Email and WebSecurity Appliance (CEF)
- McAfee Web Gateway
- Proofpoint Enterprise Protection and Enterprise Privacy
- Puresight Content Filter
- Secure Computing Webwasher
- TrendMicro Control Manager
- TrendMicro InterScan Messaging Security (Control Manager)
- TrendMicro InterScan Web Security (Control Manager)

### DAM/DB Security
- Application Security DBProtect – (CEF)

- IBM Guardium – (CEF)
- Imperva SecureSphere – (CEF)
- Oracle (Secerno DataWal) – (CEF)
- Sentrigo HedgeHog (Enterprise, vPatch) – (CEF)

### Database
- IBM DB2
- IBM DB2 UDB Audit File, version 10
- Microsoft SQL
- Oracle
- Oracle Audit Vault
- Oracle Audit Syslog, version 11gR2
- Oracle Audit XML11gR2
- Sybase Adaptive Server Enterprise

### Data Leak Prevention
- Fidelis XPS – (CEF)
- GTB Inspector – (CEF)
- McAfee Host Data Loss Prevention Endpoints (HDLP)
- Symantec DLP (Vontu)

### Data Security
- Cyber-Ark PIM – (CEF)
- Cyber-Ark PIM – (Action)
- Ingrian
- Vormetric Data Security Manager
- JBoss Security Auditing File 7.1

### Firewall
- Check Point FW-1
- Cisco PIX Firewall
- Cisco PIX/ASA Syslog, version 8.5, 8.6
- CyberGuard Firewall
- F5 BIG-IP Application Security Manager – (CEF)
- Juniper Networks (Altor Networks Virtual Firewall) – (CEF)
- Juniper Network Security Manager (NetScreen)
- Juniper Network Security Manager Syslog, version 2011.4
- Juniper Networks Firewall and VPN
- Lucent Managed Firewall
- McAfee Desktop Firewall
- Secure Computing Gauntlet Firewall/VPN
- Stonesoft Stonegate
- Symantec Enterprise Firewall
- Symantec Gateway Security
## Honeypot
- HoneyD

## IDS/IPS – Host Based
- Cisco Security Agent (Okena)
- ISS Black Ice Server Protection (SiteProtector)
- McAfee Host IPS (Entercept)
- NFR Security HID
- Symantec Critical System Protection database
- Symantec ITA (Intruder Alert)
- Tripwire Manager & Tripwire Enterprise – (CEF)

## IDS/IPS – Network Based
- Broadweb Netkeeper
- Bro IDS
- Cisco IPS Sensor
- Cisco Secure IDS
- CounterSnipe
- Enterasys Dragon
- HP-TippingPoint UnityOne SMS
- Intrusion SecureNet Pro
- ISS RealSecure Server Sensor
- ISS RealSecure WorkGroup Manager
- ISS Proventia IPS Appliance (SiteProtector)
- Juniper Networks IDP (NetScreen)
- McAfee Network Security Manager (IntruShield)
- NFR Central Management Server
- NFR Security NID
- NitroSecurity IPS
- PacketAlarm IDS
- Radware DefensePro
- Snort Sourcefire Intrusion Sensor
- Sourcefire Defense Center Management Console
- Sourcefire Defense Center eStreamer, version 5.0.2, 5.1
- Sourcefire RNA Sensor (Real-time Network Awareness)
- Symantec ManHunt
- Symantec Network Security 7100
- Topplayer Attack Mitigator

## IDM, IAM & Identity Security
- ActivCard AAA Server DB
- Beyond Trust PowerBroker Unix/Linux – (CEF)
- CA eTrust SiteMinder (Netegrity)
- Cisco Secure Access Control Server (ACS)
- Cyber-Ark PIM Suite – (CEF)
- FOXI ServerControl (CEF)
- IBM Tivoli Access Manager
- Juniper SBR (Steel Belted Radius)
- Lieberman Software ERPM – (CEF)
- Microsoft Active Directory
- Microsoft Forefront
- Microsoft Network Policy Server (Windows IAS/RADIUS)
- Novell Nsure Audit
- Oracle NetPoint (Oblix)
- Oracle SunONE Directory Server
- PacketMotion PacketSentry – (CEF)
- Ping Identity PingFederate – (CEF)
- RSA Authentication Manager (ACE Server)
- RSA Access Manager (ClearTrust)
- Secure Computing SafeWord PremierAccess
- Thycotic Secret Server – (CEF)

## Integrated Security
- Barracuda Networks Spam Firewall
- Cisco ASA 5500
- Fortinet FortiGate
- iPolicy Intrusion Prevention Firewall
- Palo Alto Networks PAN-OS - (CEF)
- Secure Computing Sidewinder
- SonicWALL
- Stonesoft StoneGate – (CEF)

## IT Operations
- HP Operations Manager (OM, OMI)
- HP Openview Operations (OVO)

## Log Consolidation & Analysis
- Cisco MARS
- Enterprise IT Security SF-RiskSaver – (CEF)
- Quest InTrust (Ika Aelita Event Manger (AEM)
- Qualys QualysGuard File, version 7.1

## Mail Filtering
- Cisco Ironport Email Security Appliance
- McAfee Email Gateway (Secure Computing IronMail)
- McAfee Security for Email Servers (GroupShield)
- MessageGate
- Symantec Messaging Gateway (Mail Security 8200 Series)

## Mainframe
- CA Top Secret
- Enterprise IT Security SF-Sherlock – (CEF)
- Enterprise IT Security SF-NoEvasion – (CEF)
- IBM OS/390 (NVAS)
- IBM OS/390 (SDSF)
- Type80 SMA_RT for RACF
- Type80 SMA_RT for CA Top Secret

## Mail Server
- IBM Lotus Notes Domino Enterprise Server
- Microsoft Exchange
- Microsoft Forefront for Exchange Server
- Sendmail

## Malware Detection
- Damballa CSP – (CEF)
- Damballa Failsafe – (CEF)
- FireEye MPS – (CEF)
- Guidance Encase – (Action)
- HBGary Active Defense – (CEF)
- Mandiant Intelligent Response – (CEF, Action)
- Taasera NetAnalyzer – (CEF)
- Truimfant Resolution Manager – (CEF)

## Midrange Systems
- IBM AS/400

## Network Access Control
- ForeScout CounterACT – (CEF, Action)
- Mirage Networks Counterpoint

## Network Behavior Anomaly
- Arbor Networks Peakflow
- Lancope StealthWatch – (CEF)
- Mazu Profiler

## Network Discovery
- Lumet IPsonar

## Network Forensics
Network Management
Cisco Works
F5 BigIP – (CEF)
HP Network Node Manager i (NNMi)

Network Monitoring
ISC DHCP
ISC BIND
Microsoft Operations Manager DB (MOM)
Microsoft System Center Operations Manager DB (SCOM)
Microsoft DHCP
Microsoft DNS
Microsoft WINS
Nagios

Network Traffic Analysis
Cisco NetFlow / Flexible Netflow
NetScout nGenius – (CEF)
nPulse HammerHead – (Action)
QoSient Argus
InMon sFlow
Ixia Net Tool Optimizer – (Action)
Solera Networks – (Action)
TCP Dump

Network Traffic Management
Cisco Distributed Director 4500
Bro IDS

Operating Systems
IBM AIX Operating System
HP OpenVMS
HP-UX Operating System
HP-UX Syslog, version 11i v3
Microsoft Windows Event Log – Unified, SQL Server 2012 for SQL Server Audit
Redhat Linux
Snare for Microsoft Windows
Solaris BSM
UNIX
Sabernet NT Syslog
HP NonStop Servers (XYPRO Merged Audit) – (CEF)

Physical Systems/Security
RedCloud Security Enterprise/Virtual – (CEF)

Policy Management
McAfee Policy Auditor
NetIQ Security Manager
SecureVantage
Solsoft Policy Server

Router
Cisco Router
Juniper Router (JUNOS)
HP H3C Comware Platform

Security Management
Enterasys Dragon Server

IBM SiteProtector
Intrusion Securenet Provider
ISS Site Protector
McAfee ePO
McAfee Rogue System Detection (via ePO)
MicroSoft Audit Collection System
Redseal Networks Advisor - (CEF)
Symantec ESM
Symantec SESA

Storage
NetApp Filer (FAS)
EMC Celerra

Switch
Cisco Catalyst
Cisco CSS 11500 Series Content Services Switches
Cisco NX-OS
Foundry Networks Big Iron
HP Ethernet Switch

Virtualization
CounterTack Event Horizon - (CEF)
VMWare ESX/ESXi Server
VMWare Virtual Center

VPN
Alcatel Secure VPN Gateway
Check Point VPN-1
Cisco VPN Concentrator
Citrix Access Gateway
Juniper/NetScreen (Neoteris) SSL VPN
Nortel Contivity Extranet Switch

Vulnerability Assessment
eEye REM Security Management Console
eEye Retina Network Security Scanner
Harris STAT Scanner
ISS Internet Scanner
McAfee Vulnerability Manager (Foundscan)
nCircle IP360 Device Profiler
nCircle IP360 Threat Monitor
Nmap
OVAL
Qualys Guard
Rapid 7 NeXpose
Symantec NetRecon
Tenable Nessus
Visionael Security Audit
Saint Vulnerability Scanner

Web Cache
BlueCoat Proxy SG Series
Microsoft ISA
Network Appliance NetCache
Squid

Web Filtering
Cisco Ironport Web Security Appliance
Websense Web Security Suite

Web Server
Apache
Microsoft IIS
Sun ONE
Wireless
AirDefense Guard
AirMagnet Enterprise
AirPatrol Wireless Policy Manager – (CEF)
AirPatrol Zone Defense (CEF)
AirTight Spectra Guard – (CEF)

Aruba Mobility Controller
Cisco AIRONET 1200
Cisco Mobility Services Engine
Newbury Networks Wi-fi Watchdog

Note: Most ArcSight SmartConnectors can be deployed as software and are also supported on ArcSight Connector Appliance

About HP ArcSight:

HP ArcSight is a leading global provider of cyber-security and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the HP ArcSight Security Information and Risk Management (SIRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cyber-theft, cyber-fraud, cyber-warfare and cyber-espionage.

For more information, visit http://www.hpenterprisesecurity.com