The HP ArcSight library of out of the box SmartConnectors provides source-optimized collection for 300+ 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, testing and certification of “CEF” (Common Event Format) for event collection, and “Action” connectors for response-actions are handled by the HP Enterprise Security Technology Ecosystem Alliances Program, which ensures further interoperability. Ecosystem partners who have achieved interoperability certification for CEF and Actions are noted below with a (CEF) or (Action) after the product name. Common Event Format (CEF) is an open standard adopted by numerous partners to make their products consumable within the ArcSight platform.

**Anti-Virus/Anti-Spam**
- F-Secure Anti-Virus
- Kaspersky Anti-Virus
- McAfee VirusScan Enterprise
- Sophos
- Sybari Antigen for Microsoft Exchange
- Symantec EndPoint Protection
- 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 – (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 Guardian – (CEF)
- Imperva SecureSphere – (CEF)
- Oracle (Secerno DataWall) – (CEF)
- Sentrigo HedgeHog (Enterprise, vPatch) – (CEF)

**Database**
- IBM DB2
- Microsoft SQL
- Oracle
- Oracle Audit Vault
- Sybase Adaptive Server Enterprise

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

**Data Security**
- Cyber-Ark Inter-Business Vault – (CEF)
- Cyber-Ark Sensitive Document Vault – (CEF)
- Ingrian
- Vormetric Data Security Manager

**Firewall**
- Check Point FW-1
- Cisco PIX Firewall
- CyberGuard Firewall
- F5 BIG-IP Application Security Manager – (CEF)
- Juniper Networks (Alt Or Networks Virtual Firewall) - (CEF)
- Juniper Network Security Manager (NetScreen)
- 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
- SANA Primary Response
- Symantec Critical System Protection
- 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 IDS  
PacketAlarm IDS  
Radware DefensePro  
Snort  
Sourcefire Intrusion Sensor  
Sourcefire Defense Center Management Console  
Sourcefire RNA Sensor (Real-time Network Awareness)  
Symantec ManHunt  
Symantec Network Security 7100  
Toplayer Attack Mitigator  

**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 – (Action)  
HBGary Active Defense – (CEF)  
Mandiant Intelligent Response – (CEF, Action)  
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**

Narus Insight CyberProtection – (CEF)  
Niksun NetDetector – (CEF)  
RSA NetWitness – (CEF)  

**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  

**Integrated Security**

ActivCard AAA Server DB  
CA eTrust SiteMinder (Netegrity)  
Cisco Secure Access Control Server (ACS)  
Cyber-Ark PIM Suite – (CEF)  
FOXT ServerControl (CEF)  
IBM Tivoli Access Manager  
Juniper SBR (Steel Belted Radius)  
Liebermann 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)  

**IT Operations**

HP Operations Manager (OM, OMi)  
HP Openview Operations (OVO)  

**Log Consolidation & Analysis**

Cisco MARS  
Quest InTrust (fka Aelita Event Manger (AEM)  
Enterprise IT Security SF-RiskSaver – (CEF)
Network Traffic Analysis
Cisco NetFlow / Flexible Netflow
NetScout nGenius – (CEF)
nPulse HammerHead – (Action)
QoSient Argus
InMon sFlow
Solera Networks – (Action)
TCP Dump

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

Physical Systems/Security
RedCloud (Plasec) – (CEF)

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

VPN
Cisco Distributed Director 4500
Bro IDS

Operating Systems
IBM AIX Operating System
HP OpenVMS
HPUX Operating System
Redhat Linux
Snare for Microsoft Windows
Solaris BSM
UNIX
Sabernet NT Syslog
HP NonStop Servers (XYPRO Merged Audit) – (CEF)
Snare
for Microsoft Windows
Solaris BSM
UNIX
Sabernet NT Syslog
HP NonStop Servers (XYPRO Merged Audit) – (CEF)

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

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

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

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
Symantec ESM
Symantec SESA

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

Switch
Cisco Catalyst
Cisco CSS 11500 Series Content Services Switches

Web Server
Apache
Microsoft IIS
Sun ONE

Storage
NetApp Filer (FAS)
EMC Celerra

Wireless
AirDefense Guard
AirMagnet Enterprise
AirPatrol Wireless Locator System (WLS) – (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 cybersecurity 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 cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit http://www.hpenterprisecurity.com/.