Hewlett Packard Enterprise

HPE ArcSight Connector supported products

The HPE ArcSight library of out-of-the-box connectors provides source-optimized collection for leading security commercial products. These products span the entire stack of event-generating source types, from network and security devices to databases and enterprise applications.

In addition to connectors developed and maintained by HPE ArcSight, we test and certify the following connector types through our technology alliances program (TAP):

- **Common event format (CEF) certified**—helps ensure event information is captured properly in the CEF
- **Action certified**—allows for control of a vendor's technology from within the HPE ArcSight console
- **Forwarding connector**—allows for events to be forwarded from ArcSight to partner solution
- **Please refer to the index section for listing by connector type**

HPE ArcSight Connector supported platform for installation

- CentOS 6.5, 6.6, 6.7, 7.0, and 7.1
- Microsoft® Windows Server® 2008 SP1/SP2 32- and 64-bit
- Microsoft Windows Server 2008 R2/R2 SP1 64-bit
- Microsoft Windows Server 2012 Standard 64-bit, R2 64-bit
- Red Hat® Enterprise Linux® (RHEL) 6.5, 6.6, 6.7, 7.0, and 7.1 64-bit
- SUSE Linux Enterprise Server 11 64-bit
- Oracle Solaris 11/(10/11-Sparc) 64-bit

Anti-virus/Anti-spam

- F-Secure Anti-Virus
- Kaspersky Anti-Virus
- Intel® (McAfee®) VirusScan Enterprise via (ePO)
- Sophos
- Symantec Endpoint Protection Manager (SEPM) database
- Symantec Mail Security for Microsoft Exchange
- Trend Micro (TM) OfficeScan (Control Manager and TM Control Manager Database DB)

Applications

- ERPScan Security Monitoring Suite for SAP®
- ESNC Security Suite-Enterprise Threat Monitoring
- IBM WebSphere
- iT-CUBE agileSI SAP
- Oracle WebLogic Server
- SAP enterprise resource planning (ERP)
- Microsoft SharePoint server database

Application security

- Bit9 + Carbon Black security platform
- CA Layer 7 SecureSpan/CloudSpan CloudControl Gateway
- Intralinks VIA
- Intel (McAfee) Application Control (Solidcore) via (ePO)
- RSA Web Threat Detection Clinical/ Healthcare applications
- FairWarning

Cloud
- Adallom Cloud Access Security Broker
- AWS Identity and Access Management (IAM)
- AWS Elastic Compute Cloud (EC2)
- AWS CloudTrail
- Box
- Blue Coat (Elastica) CloudSOC
- CloudPassage Halo
- Exabeam User Behavior Analytics
- FlexConnector for REST (can support Box, SFDC, Google™ Apps, and more)
- Illumio Policy Compute Engine (PCE)
- Microsoft Office 365
- Palerra LORIC
- vArmour Distributed Security System (DSS)
- Zscaler Nanolog Streaming Service (NSS)

Content security
- Gemalto (SafeNet) eSafe Gateway
- Barracuda Web Application Firewall (NetContinuum)
- Intel (McAfee) Email and Web Security Appliance
- Intel (McAfee) Web Gateway (Webwasher)
- Proofpoint Enterprise Protection and Enterprise Privacy
- PureSight Content Filter
- Trend Micro Control Manager
- Trend Micro InterScan Messaging Security (Control Manager)
- Trend Micro OfficeScan Client/Server (Control Manager)
- Trend Micro ScanMail for Lotus Domino (Control Manager)

Database activity monitoring (DAM)/ Database security
- Trustwave Application Security DbProtect
- IBM InfoSphere Guardium
- Imperva SecureSphere
- Intel (McAfee) Sentrigo Hedgehog (Enterprise and vPatch)
- Varonis DatAdvantage

Database
- Microsoft SQL
- Oracle Audit DB
- Oracle Audit Vault
- Oracle Audit Syslog
- Oracle Audit XML File
- Oracle Unified Audit Trail DB
- Sybase Adaptive Server Enterprise

Data leak prevention
- Fidelis Cybersecurity XPSGTB Inspector
- Intel (McAfee) Host Data Loss Prevention (HDLP) via (ePO)
- Digital Guardian

Data security
- Absolute Data and Device Security (DDS)
- Cisco ISE
- Cisco Firepower Management Center
- HPE Atalla IPC
- HPE Atalla Network Security Processor (NSP)
- JBoss Security Auditing File
- Thales Data Firewall (Vormetric)
- Zettaset BDEncrypt

Firewall
- Check Point FireWall-1 GX
- Cisco PIX/ASA Firewall
- Dell SonicWALL Firewall Syslog
- Juniper Networks (Altor Networks Virtual Firewall)
- Juniper Networks Security Manager (NetScreen)
- Juniper Networks Firewall and VPN
- Trend Micro (TippingPoint) Next-Generation Firewall (NGFW)

IDS/IPS
- BroadWeb NetKeeper
- Bro IDS
- Bro IDS NG File
- Cisco Secure IPS SDEE
- Cisco IBM AIX Management Center
- Extreme Networks Dragon IDS
- Extreme Networks Dragon Export Tool
- Trend Micro (TippingPoint) Security Management System (SMS)
- IBM Site Protector DB
- Intel (McAfee) Host Intrusion Prevention Systems (HIPS) via (ePO)
- LightCyber Magna
- NitroSecurity Syslog
- Radware DefensePro
- Snort

IDM, IAM, and identity security
- RSA Aveksa
- Bay Dynamics, Risk Fabric
- Balabit Shell Control Box
- BeyondTrust's PowerBroker
- CA SiteMinder Single Sign-On File
- CA SiteMinder Single Sign-on File
- Cisco Secure Access Control Server (ACS)
- CyberArk Privileged Account Security Management (PSM) Suite
- CyberArk Privileged Threat Analytics (PTA)
- Dell Change Auditor DB (Quest)
- Hexadite AIRS
- IBM Tivoli Access Manager
- Juniper Steel-Belted Radius (SBR)
- Lieberman Software Enterprise Random Password Manager (ERPM)
- Microsoft Active Directory
- Microsoft Forefront
- Microsoft Forefront database
- Microsoft Network Policy Server
- Netwrix Auditor
- Novell Nsure Audit
- ObserveIT Enterprise
- Oracle Sun ONE Directory Server
- Proofpoint NetCitadel ThreatOptics
- VMware® PacketMotion PacketSentry
- RSA Authentication Manager
- Securonix RTI—Risk and Threat Intelligence

- SpectorSoft Spector 360 Export Service
- Swimlane
- Thycotic Secret Server

Integrated security
- Cisco ASA 5500
- Fortinet FortiGate
- Trend Micro (TippingPoint) Next-Generation Firewall (NGFW)
- Palo Alto Networks PAN-OS
- Dell SonicWALL

IT operations
- HPE Operations Manager (OM) and HPE Operations Manager i (OMi)

Log consolidation and analysis
- Dell InTrust database
- Qualys QualysGuard

Mail filtering
- Cisco Email Security Appliance (formerly IronPort)
- Intel (McAfee) Email Gateway (Secure Computing IronMail)
- Intel (McAfee) Security for Microsoft Exchange (MSME) via (ePO)
- PhishMe Triage
- Symantec Messaging Gateway

Mainframe
- CA Top Secret
- IBM z/OS System Display and Search Facility (SDSF)
- IBM z/OS (SDSF)
- IBM z/OS (RACF)
- IBM z/OS System Log
- IBM eServer iSeries Audit Journal File
- HelpSystems PowerTech Interact
- Type80 SMA_RT for RACF

Mail server
- IBM Lotus Domino database
- Microsoft Exchange
- Microsoft Exchange PowerShell
- Microsoft Forefront Protection 2010 for Exchange Server
- Microsoft Forefront Protection Server Management Console Database
- Sendmail

Malware detection
- AhnLab Malware Defense System (MDS)
- CounterTack Active Defense (formerly ManTech)
- Damballa CSP
- Damballa Failsafe
- FireEye Malware Protection System (MPS)
- FireEye Mandiant Intelligent Response
- Fidelis Cybersecurity CIRT
- Guidance EnCase
- Lastline Enterprise anti-malware

Network access control
- HPE Aruba ClearPass
- ForeScout CounterACT
- Niara Security Intelligence
- Portnox

Network behavior anomaly
- Arbor Networks Peakflow
- IP Flow Information Export
- Qosmos DeepFlow Probes

Network forensics
- Narus nSystem
- RSA NetWitness
- ReversingLabs N1000 appliance

Network management
- Cisco Wireless LAN Controller Syslog
- HPE Network Node Manager i (NNMi) SNMP
- Lumeta Enterprise Situational Intelligence (ESI)

Network monitoring
- ISC DHCP
- ISC BIND
- Microsoft Operations Manager Database
- Microsoft System Center Operations Manager (SCOM) Database
- Microsoft System Center Configuration Manager (SCCM) Database
- Microsoft DHCP
- Microsoft DNS
- Microsoft WINS
- Radware Inflight
- Reservoir Labs R-Scope

Network traffic analysis
- Blue Coat (Solera) DeepSee
- Cisco NetFlow/Flexible NetFlow
- Corvil network data analytics
- FireEye nPulse HammerHead
- Gigamon NetFlow
- InMon sFlow®
- Intel (McAfee) Rogue System Detection via (ePO)
- NetScout nGenius
- QoSient Argus
- Seculert Automated Attack Detection Platform
- Savvius Omni Distributed Analysis Platform
- TCPdump
- Vectra Networks X-Series

Network traffic management
- Cisco Catalyst Switches

Operating systems
- IBM AIX Operating System
- HPE OpenVMS
- HP-UX operating system
- HP-UX Syslog
- Linux SUSE
- Microsoft Windows® Vista 7, 8, and 10
- Microsoft Windows Servers 2003/2008/2008 R2/2012/2012 R2
- Red Hat Linux
- Snare for Microsoft Windows
- Oracle Solaris
- UNIX®
- SaberNet NTSyslog
- HPE NonStop servers (XYGATE Merged Audit)

Packet capture
- Ixia net tool Optimizer

Policy management
- Intel (McAfee) Policy Auditor via (ePO)
- NetIQ Security Manager

Router
- Cisco Routers
- Juniper Routers (Junos)
- HPE H3C Comware Platform

Security management
- IBM Security SiteProtector
- PhishMe Intelligence
- Intel (McAfee) ePolicy Orchestrator (ePO)
- Microsoft Audit Collection System ACS DB

Server
- HPE ProLiant Gen8 Server with HPE iLO Management Engine

Storage
- Bloombase StoreSafe
- Hadoop DFS with CEF
- HPE c7000 VCM syslog
- NetApp filer (NAS)
- EMC Celerra/VNXe Storage Systems

Switch
- Cisco Content Services Switches (CSS)
- Cisco NX-OS
- Brocade BigIron (Foundry Networks)
- HPE Networking syslog

Threat management
- VarySys PacketAlarm

Threat intelligence
- Anomali's ThreatStream optic
- Comilion Instance
- FireEye (iSIGHT) ThreatScape API
- LookingGlass ScoutVision
- Recorded Future: Real-Time Threat Intelligence
- ThreatConnect Threat Intelligence Platform

Virtualization
- CounterTack Event Horizon
- McAfee Management for Optimized Virtual Environments (MOVE) via (ePO)
- VMware® ESX®/VMware® ESXi™ server
- VMware Virtual Center

VPN
- Check Point VPN-1
- Cisco VPN Concentrator
- Citrix® NetScaler
- Nortel Contivity VPN Switch
- Pulse Secure Pulse Connect Secure

Vulnerability assessment
- eEye REM Security Management Console
- eEye Retina Network Security Scanner
- FFRI FFR yarai
- Intel (McAfee) Vulnerability Manager (FoundScan)
- Belden (Tripwire) IP360 Device Profiler
- Belden (Tripwire) IP360 Threat Monitor
- Lumension PatchLink Scanner DB
- Nmap
- Open Vulnerability and Assessment Language (OVAL) standard
- Rapid7 Nexpose
- SOC Prime Integration Framework
- Squid Web Proxy Cache
- Tenable Nessus
- SAINT Vulnerability Scanner
- Webroot BrightCloud

Web cache
- Blue Coat ProxySG series
- Microsoft Internet Security and Acceleration (ISA) Server

Web filtering
- Cisco IronPort Web Security Appliance
- McAfee SiteAdvisor Enterprise via ePO
- Forcepoint (Websense) Web Security Suite

Web server
- Apache
- Microsoft Internet Information Services (IIS)
- Oracle Sun ONE

Wireless
- AirMagnet Enterprise
- Cisco Mobility Services Engine
- Cisco NetFlow/Flexible NetFlow
- Cisco NX-OS
- Mojo Networks AirTight Management Console
- Zebra AirDefense Guard

HPE ArcSight index listing of connectors available today

- Apache
- Arbor Networks TMS (Formerly TMS Peakflow)
- AWS CloudTrail
- AWS EC2
- AWS IAM
- Barracuda Web Application Firewall (NetContinuum)
- Belden (Tripwire) IP360 Device Profiler
- Belden (Tripwire) IP360 Threat Monitor
- Blue Coat ProxySG series
- Box
- Brocade BigIron (Foundry Networks)
- Bro IDS
- Bro IDS NG File
- BroadWeb NetKeeper
- CA SiteMinder Single Sign-On File
- CA SiteMinder Single Sign-on File
- CA Top Secret
- CentOS
- Check Point FireWall-1 GX
- Check Point VPN-1
- Cisco Secure IPS SDEE
- Cisco ASA
- Cisco Catalyst Switches
- Cisco CSS
- Cisco Email Security Appliance (formerly IronPort)
- Cisco IronPort Web Security Appliance
- Cisco PIX Firewall
- Cisco Routers
- Cisco ISE
- Cisco Wireless LAN Controller Syslog
- Dell (Quest) Change Auditor DB
- Dell (Quest) InTrust (fka AEM)
- Dell SonicWALL Firewall Syslog
- eEye REM Security Management Console
- eEye Retina Network Security Scanner
- EMC Celerra/VNXe Storage Systems
- Extreme Networks Dragon IDS
- Extreme Networks Dragon Export Tool
- FlexConnector for REST (can support Box, SFDC, Google Apps, and more)
- F-Secure Anti-Virus
- Gemalto (SafeNet) eSafe Gateway
- HPE Aruba WLAN Mobility Controller
- HPE H3C Comware Platform
- HPE Network Node Manager i (NNMi) SNMP
- HPE Networking syslog
- HPE OpenVMS
- HP-UX Syslog
- IBM AIX Operating System
- IBM Domino database
- IBM Domino Web server
- IBM Site Protector DB
- IBM Security SiteProtector System
- IBM Tivoli Access Manager
- IBM WebSphere
- Intel (McAfee) Application Control (Solidcore) via (ePO)
- Intel (McAfee) Email Gateway (Secure Computing IronMail)
- Intel (McAfee) Firewall Enterprise
- Intel (McAfee) Host Data Loss Prevention (HDLP) via (ePO)
- Intel (McAfee) Host Intrusion Prevention Systems (HIPS) via (ePO)
- Intel (McAfee) Policy Auditor via (ePO)
- Intel (McAfee) Rogue System Detection via (ePO)
- Intel (McAfee) Security for Microsoft Exchange (MSME) via (ePO)
- Intel (McAfee) VirusScan Enterprise via (ePO)
- Intel (McAfee) Vulnerability Manager (FoundScan)
- Intel (McAfee) Web Gateway (Webwasher)
- IP Flow Information Export
- ISC BIND
- ISC DHCP
- JBoss Security Auditing File
- Juniper Networks Security Manager (NetScreen)
- Juniper Networks Firewall and VPN
- Juniper Routers (Junos)
- Juniper SBR
- Kaspersky Anti-Virus
- Linux SUSE
- Lumension PatchLink Scanner DB
- Microsoft Active Directory

HPE ArcSight index listing of connectors available today (continued)

- Microsoft ACS database
- Microsoft DHCP
- Microsoft DNS
- Microsoft Exchange
- Microsoft Exchange PowerShell
- Microsoft Forefront
- Microsoft Forefront DB
- Microsoft Forefront Protection Server Management Console DB
- Microsoft Forefront Protection 2010 for Exchange Server
- Microsoft ISA
- Microsoft Network Policy Server (Windows IAS/RADIUS)
- Microsoft Office 365
- Microsoft Operations Manager database
- Microsoft SharePoint server database
- Microsoft SQL
- Microsoft SCCM database
- Microsoft SCOM database
- Microsoft Windows 7/8/2003/XP/2008 Server/Vista
- Microsoft Windows Servers 2003/2008/2008 R2/2012/2012 R2
- Microsoft WINS
- FAS should be (NAS)
- NetIQ Security Manager
- NitroSecurity Syslog
- Nmap
- Nortel Contivity VPN Switch
- Novell Nsure Audit
- Oracle Audit DB
- Oracle Audit Syslog
- Oracle Audit Vault
- Oracle Audit XML File
- Oracle Solaris
- Oracle Sun ONE
- Oracle Sun ONE Directory Server
- Oracle WebLogic Server
- OVAL standard
- Proofpoint Enterprise Protection and Enterprise Privacy
- Pulse secure Pulse Connect Secure
- PureSight Content Filter
- QoSient Argus
- Qualys QualysGuard
- Radware DefensePro
- Rapid7 Nexpose
- Red Hat Linux
- RSA Authentication Manager
- SaberNet NTSyslog
- SAINT Vulnerability Scanner
- SAP ERP
- Snare for Microsoft Windows
- Snort
- Sophos
- Squid Web Proxy Cache
- Sybase Adaptive Server Enterprise
- SEPM database
- Symantec Mail Security for Microsoft Exchange
- Symantec Messaging Gateway
- TCPdump
- Tenable Nessus
- Trend Micro Control Manager
- Trend Micro InterScan Messaging Security (Control Manager)
- Trend Micro OfficeScan Client/Server (Control Manager)
- Trend Micro ScanMail for Domino (Control Manager)
- Trend Micro (TippingPoint) Security Management System (SMS)
- UNIX
- VarySys PacketAlarm
- VMware ESX/ESXi server
- VMware Virtual Center
- Forcepoint (Websense) Web Security Suite
- Zebra AirDefense Guard

Action-certified solutions

- Absolute Data and Device Security (DDS)
- Aruba ClearPass
- Cisco Firepower Management Center
- Comilion Instance
- CyberArk PSM Suite
- Digital Guardian
- FireEye Mandiant Intelligent Response
- FireEye Network Forensics Platform (PX)
- ForeScout CounterACT
- General Dynamics CIRT
- Guidance EnCase
- IBM Resilient Systems Incident Response Platform
- Ixia Net Tool Optimizer
- Niara Security Intelligence
- NIKSUN NetOmni
- Proofpoint NetCitadel ThreatOptics
- RSA Aveksa
- Securonix Risk and Threat Intelligence RTI
- Symantec Security Analytics (Solera DeepSee)
- vArmour Analytics Platform

Forwarding-certified solutions

- Bay Dynamics Risk Fabric
- Exabeam User Behavior Analytics
- Hexadite AIRS
- Niara Security Intelligence
- Palerra LORIC
- Savvius Omni Distributed Analysis Platform
- Swimlane

HPE ArcSight CEF connectors index listing

CEF-certified solutions:

- ABAP-Experts SecurityBridge
- AhnLab Malware Defense System (MDS)
- Anomali's ThreatStream OPTIC
- Aruba ClearPass
- Arxan GuardIT
- Avigilon Access Control Manager (ACM)
- Ayehu eyeShare
- Balabit Shell Control Box
- Belden (Tripwire Enterprise)
- BeyondTrust's PowerBroker
- Bit9 + Carbon Black Security Platform
- Bloombase StoreSafe
- Bomgar Privileged Access Management
- Bricata ProAccel
- Brinqa Risk Analytics
- Bromium Advanced Endpoint Security
- CA Technologies SecureSpan/CloudSpan CloudControl Gateway
- CA Technologies Privileged Access Management
- Cilasoft QJRN/400
- Cisco Firepower Management Center
- CloudPassage Halo
- Comilion Instance
- CorreLog Syslog Defender
- Corvil Network Data Analytics
- CounterTack Sentinel (Event Horizon)
- CounterTack Active Defense (formerly ManTech)
- CyberArk Privileged Account Security Management (PSM) Suite
- CyberArk Privileged Threat Analytics (PTA)
- Damballa CSP
- Damballa Failsafe
- Digital Guardian
- E8 Security Behavioral Intelligence Platform Application
- Edge Technologies AppBoard and enPortal
- Endgame
- ERPScan Security Monitoring Suite for SAP
- ESNC Security Suite-Enterprise Threat Monitoring
- F5 Big-IP Advanced Firewall Manager (AFM)
- FairWarning
- FFRI FFR yarai
- Fidelis Cybersecurity XPS
- FireEye Malware Protection System (MPS)
- FireEye Mandiant Intelligent Response
- FireEye (iSIGHT) ThreatScape API
- ForeScout CounterACT
- Fortinet FortiGate
- General Dynamics CIRT
- Gigamon GigaVUE/GigaSECURE
- GTB Technologies Inspector
- Gurucul Analytics Platform
- Hexadite AIRS
- HelpSystems PowerTech Interact
- HPE Aruba ClearPass
- HPE Atalla IPC
- HPE Atalla Network Security Processor (NSP)
- HPE NonStop servers (XYGATE Merged Audit) (XMA)
- IBM InfoSphere Guardium
- Illumio Policy Compute Engine (PCE)
- Illusive Networks
- Imperva SecureSphere

HPE ArcSight CEF connectors index listing (continued)

- Indegy Industrial Cyber Security Platform
- Intel (McAfee) Email and Web Security Appliance
- Intel (McAfee) Sentrigo Hedgehog (Enterprise and vPatch)
- Intel (McAfee) StoneSoft StoneGate Firewall
- Intralinks VIA
- iT-CUBE agileSI SAP
- Juniper Networks Altor Networks Virtual Firewall
- Lancope StealthWatch
- Lastline Enterprise Anti-Malware Solution
- Lieberman Software ERPM
- LightCyber Magna Platform
- LookingGlass Cyber Solutions ScoutVision
- Lumeta Enterprise Situational Intelligence (ESI)
- Lumeta IPsonar
- Microsoft (Adallom) Cloud Access Security Broker
- Mojo Networks AirTight Management Console
- NetScout Systems nGenius Performance Manager
- Netwrix Auditor
- Nexthink Engine
- Niara Security Intelligence
- NIKSUN NetDetector
- ObserveIT Enterprise
- Palerra LORIC
- Palo Alto Networks PAN-OS
- PhishMe Intelligence
- PhishMe Triage
- Portnox Network Security
- Qosmos DeepFlow Probes
- Radware Inflight
- Recorded Future Threat Intelligence Platform
- RedSeal Network and Vulnerability Advisor
- Reservoir Labs R-Scope
- ReversingLabs N1000 Appliance
- RSA NetWitness
- RSA Web Threat Detection
- SailPoint IdentityIQ
- Seculert Automated Attack Detection Platform
- Securonix Risk and Threat Intelligence (RTI)
- SOC Prime Integration Framework
- Symantec Blue Coat (Elastica) CloudSOC
- Symantec System Recovery
- Sysorex Zone Defense
- TaaSera TaaS NetAnaylzer
- ThreatConnect Threat Intelligence Platform
- Thycotic Secret Server
- TrapX DeceptionGrid
- Trend Micro Deep Security
- Trend Micro (TippingPoint) Next-Generation Firewall (NGFW)
- Trustwave Application Security DbProtect
- Type80 SMA_RT
- vArmour Analytics Platform
- Varonis DatAdvantage
- Vectra Networks X-Series
- Veriato 360 (Spector 360)
- Verodin Security Instrumentation Platform
- Vormetric Data Security Manager
- Webroot BrightCloud
- Zettaset BDEncrypt
- Zscaler Nanolog Streaming Service (NSS)

Learn more at
protect724.hpe.com

Resources

HPE ArcSight Marketplace

Sign up for updates

4AA5-3404ENW, March 2017, Rev. 9

Hewlett Packard Enterprise