FORTRA™

DATASHEET (TRIPWIRE)

Tripwire LogCenter Data Collection Capabilities

June 2023

Fortra's Tripwire® LogCenter® supports a variety of data collection methods, including agent-based collection using the Tripwire Axon® agent, and agentless collection via syslog, SNMP, WMI, file collectors and remote connectors for Cisco, Check Point and databases.

The Tripwire Axon agent included with Tripwire LogCenter supports the following platforms:

- CentOS Linux 5.3–5.11+ (32- and 64-bit)
- CentOS Linux 6.0–6.5+ (32- and 64-bit)
- CentOS Linux 7.0–7.3 (64-bit)
- Debian Linux 8.5–8.10 (32- 64-bit)
- Oracle Linux UEK 7.2–7.5 (64-bit)
- Red Hat Enterprise Linux 5.3–5.11+ (32- and 64-bit)
- Red Hat Enterprise Linux 6.0–6.6 (32- and 64-bit)
- Red Hat Enterprise Linux 7.0–7.4 (64-bit)
- SUSE Linux 11.4, 12.0–12.3 (64-bit)
- Ubuntu Linux 14.04.4 LTS and above (32- and 64-bit)
- Ubuntu Linux 16.04 LTS and above (32- and 64-bit)
- Microsoft Windows 7 (32- and 64-bit)
- Microsoft Windows 8, 8.1, 8.1 Embedded (32- and 64-bit)
- Microsoft Windows 10 (64-bit)
- Microsoft Windows Embedded POSReady 7 (32- and 64-bit)
- Microsoft Windows Server 2008 SP1, SP2 (32- and 64-bit)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2012 R2 (64-bit)
- Microsoft Windows Server 2016 R2 (64-bit)

Data collection is only part of the equation—Tripwire LogCenter normalizes the log data it collects in order to make it accessible and useful with its product capabilities of indexing, search and correlation. Tripwire LogCenter supports normalization rules for products in the following table, and Tripwire is constantly adding supported platforms.

Turning log data into information requires support for the platforms that matter to you.

Vendor	Product
A10 Networks	A10 Networks
Adiscon	EventReporter
Adtran	NetVanta
AIDE	AIDE
Alcatel	AOS
Alcatel	Wifi
Alcatel-Lucent	OmniAccess ESR Compact and Modular Routers
Anixter	Bosch IP Camera
Apache Software Foundation	Apache HTTP Server
Apache Software Foundation	Apache James Server
Apache Software Foundation	Apache log4j
Apache Software Foundation	Apache Tomcat
APC	NetBotz
APC	PDU
Apple	Mac OS
Arbiter Systems	Arbiter GPS Satellite Clock
Arbor Networks	Arbor Networks
Arbor Networks	Arbor Peakflow
Array Networks	Array Networks
Aruba Networks	Aruba Wireless
Aruba Networks	ArubaOS
Aruba Networks	ClearPass Access Management
Astaro	ASG 320 Security Gateway
AudioCodes Limited	Mediant
Avaya	Secure Router
Axis Communications	Axis
BalaBit IT Security	Syslog-ng Agent for Windows
Barracuda Networks	Barracuda Load Balancer
Barracuda Networks	Barracuda Message Archiver
Barracuda Networks	Barracuda NG Firewall
Barracuda Networks	Barracuda Web Filter
Barracuda Networks	Barracuda Web Security Gateway
BeyondTrust	Bomgar PRA
Blue Coat Systems	Blue Coat ProxyAV
Blue Coat Systems	Blue Coat ProxySG
BMC Software	Discovery
BMC Software	TrueSight Operations Management
Bro.org	Bro
Brocade	Switch
Brocade	Wireless LAN Controller
Cambium Networks	PTP Series
CentOS	CentOS
Check Point	Check Point
Check Point	Check Point CEF
Check Point	GAiA
Check Point	SmartDefense
Check Point	SmartCenter CEF
Cisco Systems	ASA (Adaptive Security Appliance)
Cisco Systems	CallManager
Cisco Systems	CatOS
Cisco Systems	Mobility Services Engine (MSE)
Cisco Systems	Secure Access Control Server (ACS)
Cisco Systems	Cisco Security Agent (CSA)
Cisco Systems	Prime Network Control System (Prime NCS)
Cisco Systems	Prime Infrastructure
Cisco Systems	Security Manager
Cisco Systems	Firepower Management Center
Cisco Systems	Firepower NGIPS
Cisco Systems	Firepower Threat Defense
Cisco Systems	FWSM (Firewall Services Module)
Cisco Systems	IMC
Cisco Systems	IOS
Cisco Systems	IPS
Cisco Systems	Ironport (ESA/WSA)
Cisco Systems	ISE
Cisco Systems	NX-OS
Cisco Systems	PIX Security Appliance
Cisco Systems	Secure IDS
Cisco Systems	VPN Series Concentrator
Cisco Systems	Wireless LAN Controller (WLC)
Citrix	Netscaler
Clavister AB	Clavister
Cloudflare	Enterprise Log Share
Computer Associates	SiteMinder Policy Server
Cordys	Cordys
Courier POP3	Courier POP3
Cybectec	SMP 16 Gateway
CyberArk	Disaster Recovery Vault
CyberArk	Enterprise Password Vault
CyberArk	Privileged Identity Management
CyberArk	Privileged Identity Management (CEF Events)
CyberGuard	CyberGuard
Debian GNU/Linux	Debian
Dell	Defender
Dell	Dell Compellent Storage Center
Dell	EMC
Dell	EMC Avamar
Dell	EMC ML3 Tape Libary
Dell	EMC PowerSwitch Series S
Dell	EMC VNXe-Unity
Dell	Equallogic
Dell	iDRAC6
Dell	iDRAC7
Dell	iDRAC9
Dell	Networking OS
Dell	PowerConnect
Digi	Digi Passport
Digi	PortServer
DigitalPersona, Inc.	Digital Persona
DLink	DLink
Docker	Docker
Duo	Authentication Proxy
Eaton Cooper	Yukon IED Manager Suite (IMS)
EMC	EMC Recoverpoint
Enterasys Networks	Dragon EMS
Enterasys Networks	Dragon HIDS
Enterasys Networks	Enterasys
ESRI	ArcGIS
Extreme Networks	Extreme XOS
Extreme Networks	ExtremeWare
F5 Networks	F5 BIG-IP
F5 Networks	F5 Firepass
FileMaker	FileMaker Server
FileZilla	FileZilla Server
FireEye	Endpoint Security
FireEye	Web MPS
FNS Bancs	FNS Bancs
Forescout	CounterACT
Forescout	Forescout
ForgeRock	openAM
Fortinet	FortiAnalyzer
Fortinet	FortiAuthenticator
Fortinet	FortiGate
Fortinet	FortiGate v4.0 MR2
Fortinet	FortiGate v4.0 MR3
Fortinet	FortiGate v5.0
Fortinet	FortiOS
Fortinet	FortiOS CEF
Fortinet	FortiWifi
Fortinet	FortiWeb
Foundry Networks	Foundry ServerIron
FreeBSD Foundation	FreeBSD
GarrettCom	INOS
GarrettCom	MNS-6K-SECURE
GarrettCom	MNS-DX
Gauntlet	Gauntlet Modem
GE	iFix
Gentoo Linux	Gentoo

Vendor	Product
GitHub	GitHub
GlobalSCAPE	GlobalScape
Guardix	Guardix
Hirschmann	Industrial Ethernet Rail Switch Power Lite
Hirschmann	Industrial Ethernet Switches
Hirschmann	Industrial Firewall
Hirschmann	Industrial HiVision
HP	3PAR
HP	Comware
HP	EVA
HP	GbE2c Ethernet Blade Switch
HP	iLO
HP	OpenVMS
HP	ProCurve
HP	SAN Switch
HP	HP-UX
HP	Onboard Administrator
HP	TippingPoint
HP	Virtual Connect
HPE (Hewlett Packard Enterprise)	ArubaOS-CX
HPE (Hewlett Packard Enterprise)	Nimble Storage
HPE (Hewlett Packard Enterprise)	Onyx
HyTrust, Inc.	HyTrust Security Appliance
IBM	AIX
IBM	AS/400
IBM	IBM WebSphere
IBM	Informix Dynamic Server
IBM Corporation	ServeRaid
IBM Internet Security Systems (ISS)	ISS
IBM Internet Security Systems (ISS)	NetworkIce
IBM Lotus Development Corporation	IBM Lotus Notes
Imperva	SecureSphere WAF
Industrial Defender	Network Intrusion Detection System (NIDS)
Infoblox Inc.	Infoblox NIOS
Informatica	Informatica PowerCenter
Ingrian Networks	IngrianNAE
Inter7	Vpopmail
Internet Systems Consortium, Inc.	Bind Linux
Internet Systems Consortium, Inc.	Bind Windows
Ipswitch	WS_FTP Server
JetBrains	TeamCity
JFrog	Artifactory
Juniper Networks	MAG Series
Juniper Networks	Juniper Netscreen
Juniper Networks	Juniper SSG-WLAN
Juniper Networks	Juniper SSL VPN
Juniper Networks	Junos OS
Juniper Networks/Pulse Secure	Juniper - Pulse Secure SSL VPN Appliances
KEMP Technologies	LoadMaster
Linksys	VPN Router
LogMeIn	LogMeIn Central
Mageia	Mageia
ManageEngine	Password Manager Pro
Mandriva S.A.	Mandriva
Marconi	Marconi
Masibus	GPS Time Sync Clocks
McAfee	McAfee Alert Manager
McAfee	McAfee DAM
McAfee	McAfee ePolicy Orchestrator (ePO)
McAfee	McAfee IntruShield
McAfee	McAfee NSM
McAfee	McAfee VirusScan
McAfee	McAfee Web Gateway
McAfee	Sidewinder
McAfee	Firewall Enterprise
Meinberg	LANTIME
Microchip	SyncServer S Series
MICROS Systems, Inc.	Micros Opera
Microsoft	BIZTalk
Microsoft	IIS Advanced Logging Module; IIS - Web/FTP
Microsoft	Microsoft Cloud App Security
Microsoft	Microsoft DHCP Server
Microsoft	Microsoft Exchange Server
Microsoft	Microsoft Forefront Threat Management Gateway
Microsoft	Microsoft Internet Authentication Service (IAS)
Microsoft	Microsoft Internet Information Server (IIS) Advanced
Microsoft	Microsoft ISA Server
Microsoft	Microsoft Operations Manager (MOM)
Microsoft	Microsoft Proxy Logs
Microsoft	Microsoft SQL Server
Microsoft	Microsoft SQL Server (CEF Events)
Microsoft	Microsoft Sysmon
Microsoft	Network Policy Server (NPS)
Microsoft	Windows
Microsoft	Windows XP-2003
Microsoft	Windows 2008, 2008 R2, 2012, Vista, 7, 8, 2016
Microsoft	Windows 10, 2019
Microsoft	Windows LTR
Microsoft	Windows NT 6
Microsoft	Windows NT 10
Microsoft	Windows 2003 Firewall
Microsoft	Windows 2008 R2 Firewall
Motorola	Motorola AirDefense
Motorola	RFS
MOXA	NPort
MySQL AB	MySQL Linux
MySQL AB	MySQL Windows
NetApp	NetApp ONTAP
NetApp	NetApp Virtual Tape Library
NetBSD	NetBSD
Netopia	Netopia
Newnet Communication Tech	AccessGuard
Nginx	Nginx
Niksun	Niksun
Nitgen	Access Manager
Node.js	Node.js
Nokia	Nokia IPSO
Nortel Networks	Nortel Connectivity
Nortel Networks	Nortel Passport
Nortel Networks	Nortel Switch
NovaTech	OrionLX
Nozomi Networks	N2OS
Nutanix	Acropolis (AOS)
One Identity	TPAM
Open Source	Kippo
Open Source	gIFTPd
Open Source	Imapd
Open Source	IPFilter
Open Source	IPTables
Open Source	ModSecurity
Open Source	Nagios
Open Source	NcFTPd
Open Source	NTP
Open Source	OpenSSH
Open Source	Postfix
Open Source	Pure-FTPd
Open Source	QMail
Open Source	Squid Cache
Open Source	TACACS+
Open Source	vsftpd
OpenBSD	OpenBSD
Oracle	Oracle
Oracle	Oracle Access Manager
Oracle	Oracle - CEF
Oracle	Oracle Database
Oracle	Oracle DB Collector
Oracle	Oracle Linux
Oracle	Oracle Web Cache

Vendor	Product
Oracle	Oracle WebLogic Server
Oracle	Siebel
OSI	Monarch
PacketMotion	PacketSentry
PADS	Pads
Palo Alto Networks	PAN-OS
Panasonic Avionics Corporation	Panasonic Avionics AI
Pentaho	Pentaho
Perle	IOLAN
Phion Firewall	Phion Netfence
PostgreSQL	PostgreSQL
Progress Software	Sonic ESB
ProofPoint	ProofPoint
QBIK	WinGate
QNAP	QTS
Quest Software	Quest Active Roles
Radware	Radware
Radware	Radware Alteon
Raritan	Dominion SX48
Red Hat	Red Hat Ansible Tower
Red Hat	Red Hat Enterprise Linux
Red Hat	Red Hat Fedora Core Linux
Riverbed	Riverbed
RSA	DLP
RSA	RSA SecurID
RuggedCom	RuggedServer, RuggedSwitch
RuggedCom	RuggedBackbone
Safend	WAVE Data Protection
SafeNet Networks	SafeNet DataSecure
SAP AG	SAP
Schneider Electric	ADAM
Schneider Electric	EcoStruxure ADMS
Schneider Electric	Modicon PAC
Schneider Electric	OASyS DNA
Schneider Electric	Remote Terminal Unit (RTU)
Secui	Secui MF2
SEL	SEL RTAC
SEL	SEL-2488
SEL	SEL-3610
SEL	SEL-3620
Sendmail	Sendmail
ServGate Edgeforce	ServGate
Shorewall	Shorewall
Siemens	RUGGEDCOM CROSSBOW
Sierra Wireless	ALEOS
Slackware Linux	Slackware
Snare	Snare AIX
Snare	Snare Apache
Snare	Snare CentOS
Snare	Snare IIS
Snare	Snare Linux
Snare	Snare Windows
Software AG	WebMethods Integration Server
SolarWinds	NetFlow
SonicWall	SonicWall
SonicWall	SonicWall Aventail E-Class SRA
Sophos	Sophos Antivirus
Sophos	Sophos Enterprise Console
Sophos	Sophos Enterprise Console (CEF Events)
Sophos	SG Series UTM
Sophos	XG Firewall
Sourcefire	Clam Antivirus
Sourcefire	Snort
Sourcefire	Sourcefire
SSH	SSH Tectia Server
SSH	SSH Tectia Server CEF
Stonesoft	Stonegate Firewall
StorMagic	SvSAN
Sun Microsystems	Solaris
Sun Microsystems	Sun ONE Web Server (iPlanet)
SUSE	SUSE Linux
SUSE	SUSE Linux Enterprise Server
SWIFT	SWIFT Alliance Access
Symantec	Symantec
Symantec	AntiVirus
Symantec	Endpoint Protection Manager
Symantec	Endpoint Protection Client
Symantec	Endpoint Protection Client - CEF
Tofino	Xenon Security Appliance
Tofino	Configurator
Top Layer Networks	TopLayer
Townsend Security	Patrick Townsend LogAgent
Transition Networks	Indura
Transition Networks	SM24TAT4XA
Trend Micro	Apex One CEF
Trend Micro	Third Brigade
Trend Micro	Tipping Point IPS
Trend Micro	Tipping Point SMS
Trend Micro	Deep Security CEF
Trend Micro	Deep Security Manager
Trend Micro	OfficeScan
Trend Micro	OSSEC
Tripp Lite	Tripp Lite B096-048
Tripwire	IP360 Device Profiler (DP)
Tripwire	IP360 VnE
Tripwire	Tripwire Configuration Compliance Manager (CCM)
Tripwire	Tripwire Enterprise
Tripwire	Tripwire Enterprise - CEF
Tripwire	Tripwire Event Sender
Tripwire	Tripwire for Servers
Tripwire	Tripwire Industrial Appliance
Tripwire	Tripwire Industrial Sentinel
Tripwire	Tripwire Industrial Visibility
Tripwire	Tripwire Industrial Visibility - Legacy
Tripwire	Tripwire LogCenter
Tripwire	Tripwire State Analyzer
Trustwave	Secure Web Gateway
Ubuntu	Ubuntu Linux
Vasco	Vasco IDENTIKEY Server
Veeam	Veeam Backup & Replication - CEF
Verifone	Sapphire
Verifone	Commander Site Controller
Veritas Technologies	Backup Exec
Veritas Technologies	System Recovery
VMware	Carbon Black App Control
VMware	Photon OS
VMware	ESX
VMware	ESXi
VMware	vCenter Server
Vyatta	Vyatta Network OS
WatchGuard	Watchguard
Wave	Wave Data Protection
Websense	Triton Security Gateway
Westell	Westell
Westermo	RedFox Industrial Series (RFI)
WU-FTPD	Wu-ftpd

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.