Security as a Service

The following data sources are supported by DeepSeas Log Analytics Platform. Support for additional data sources may be available by request or through custom integration.

Category	Type	Vendor	Version
Identity	Active Directory	Microsoft	Active Directory
Endpoint	Anti-Virus	Bitdefender	Bitdefender_AV
Endpoint	Anti-Virus	Cisco	CiscoACS_SOD
Endpoint	Anti-Virus	Cylance	Cylance
Endpoint	Anti-Virus	ESET	ESET_NOD32
Endpoint	Anti-Virus	ESET	ESET_NOD32
Endpoint	Anti-Virus	Network Associates Inc.	McAfee ePO
Endpoint	Anti-Virus	McAfee	McAfee UVScan
Endpoint	Anti-Virus	McAfee	McAfee_ePO
Endpoint	Anti-Virus	Sonicwall	Sonicwall Anti_Virus
Endpoint	Anti-Virus	Sophos	Sophos Anti-Virus
Endpoint	Anti-Virus	Trendmicro	Trendmicro Anti-Virus
Endpoint	Anti-Virus	Symantec	Crowdstrike
Endpoint	Anti-Virus	CrowdStrike	Symantec Anti-Virus Corporate Edition
Endpoint	File Integrity	Bromium	File Integrity
Endpoint	File Integrity	Carbon Black	Application Control
Endpoint	File Integrity	Trendmicro	Trendmicro FIM
Endpoint	File Integrity	Tripwire Inc	File Integrity
Endpoint	Host Intrustion & Prevention	Cisco	Cisco Security Agent
Endpoint	Host Intrustion & Prevention	Cisco	Cisco Security Agent
Endpoint	Host Intrustion & Prevention	CounterTack	Sentinel
Endpoint	Host Intrustion & Prevention	Infocyte	Hunt Server
Endpoint	Host Intrustion & Prevention	MobileIron	MBCore
Endpoint	Host Intrustion & Prevention	OSSEC	OSSEC Host IDS
Endpoint	Host Intrustion & Prevention	Sonicwall	Sonicwall HIPS

Endpoint	Host Intrustion & Prevention	Trendmicro	Trendmicro HIPS
Endpoint	Malware Protection	Cisco	AMP
Endpoint	Malware Protection	Fire_Eye	NX
Endpoint	Malware Protection	Fire_Eye	NX
Endpoint	Malware Protection	Fortinet	FortiSandbox
Endpoint	Malware Protection	Ivanti	Endpoint Security
Endpoint	Malware Protection	MalwareBytes	EndpointSecurity
Endpoint	Linux/Unix	Amazon Web Services	AWS Linux
Endpoint	Linux/Unix	Brother	Printer
Endpoint	Linux/Unix	Cisco	Cisco_UCS
Endpoint	Linux/Unix	Dell, Inc.	DELL_Server
Endpoint	Linux/Unix	Hewlett Packard	UNIX
Endpoint	Linux/Unix	IBM	AS400
Endpoint	Linux/Unix	IBM	ZOS
Endpoint	Linux/Unix	Linux	Linux
Endpoint	Linux/Unix	NetApp	OnTap Cluster
Endpoint	Linux/Unix	NetApp	OnTap Cluster
Endpoint	Linux/Unix	PureStorage	Purity NAS
Endpoint	Linux/Unix	QNAP	QNAP NAS
Endpoint	Linux/Unix	RedHat	RedHat Linux
Endpoint	Linux/Unix	Sun Microsystems	Solaris
Endpoint	Linux/Unix	SUSE	Suse Linux
Cloud	Azure	Microsoft	Azure_Administrative
Cloud	Azure	Microsoft	Azure_API_Management
Cloud	Azure	Microsoft	Azure_App_Insights
Cloud	Azure	Microsoft	Azure_Autoscale_Events
Cloud	Azure	Microsoft	Azure_Diagnostics_Events
Cloud	Azure	Microsoft	Azure_HDInsight
Cloud	Azure	Microsoft	Azure_IIS
Cloud	Azure	Microsoft	Azure_Key_Vault
Cloud	Azure	Microsoft	Azure_Kubernetes_Service_(AKS)
Cloud	Azure	Microsoft	Azure_Networking_Resources

Cloud	Azure	Microsoft	Azure_NSG_Flow_Logs
Cloud	Azure	Microsoft	Azure_OS_Logs
Cloud	Azure	Microsoft	Azure_Recommendation
Cloud	Azure	Microsoft	Azure_Security_Center
Cloud	Azure	Microsoft	Azure_Service_Alert
Cloud	Azure	Microsoft	Azure_Service_Health
Cloud	Azure	Microsoft	Azure_SQL_DB
Cloud	Azure	Microsoft	Azure_Storage_Analytics
Cloud	Azure	Microsoft	Azure_Subscription_Monitoring
Cloud	Azure	Microsoft	Azure_Virtual_Machines
Cloud	Azure	Microsoft	Azure_WAF
Cloud	AWS	Amazon Web Services	Cloud_Trail
Cloud	AWS	Amazon Web Services	Cloud_Watch
Cloud	AWS	Amazon Web Services	Config
Cloud	AWS	Amazon Web Services	Guard Duty
Web Gateway	Web Proxy	Barracuda	Barracuda_WF
Web Gateway	Web Proxy	Blue Coat Systems	BLUECOAT SG
Web Gateway	Web Proxy	Blue Coat Systems	BLUECOAT SG
Web Gateway	Web Proxy	Cisco	Cisco_WSA
Web Gateway	Web Proxy	Forcepoint	Email Gateway
Web Gateway	Web Proxy	Forcepoint	Web Security
Web Gateway	Web Proxy	Fortinet	FortiWeb
Web Gateway	Web Proxy	Iprism	Iprism_WF
Web Gateway	Web Proxy	IronPort	IronPort_ESA
Web Gateway	Web Proxy	IronPort	IronPort_WSA
Web Gateway	Web Proxy	McAfee	Email Gateway
Web Gateway	Web Proxy	McAfee	Web Gateway
Web Gateway	Web Proxy	Microsoft	Threat Management Gateway
Web Gateway	Web Proxy	PROOFPOINT	Email Security
Web Gateway	Web Proxy	Radware	DefensePro_DOS
Web Gateway	Web Proxy	Sonicwall	Web Gateway

Web Gateway	Web Proxy	Trendmicro	Web Gateway
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Zix	Email_Encryption
Web Gateway	Web Proxy	Zscaler	Nanolog
DNS	DNS	BlueCat Networks	BLUECAT
DNS	DNS	BlueCat Networks	BLUECAT
DNS	DNS	Cisco	CISCO
DNS	DNS	DNS Security	DNS
DNS	DNS	InfoBlox	InfoBlox
DNS	DNS	InfoBlox	InfoBlox
DNS	DNS	Simple_DNS	SDNS
DNS	DNS	Sonicwall	SONICWALL
DHCP	DHCP	DHCP Security	DHCP
DHCP	DHCP	Sonicwall	DHCP
Network	FireWall	Avantail	Avantail VPN
Network	FireWall	Amazon Web Services	Firewall
Network	FireWall	Barracuda	Barracuda_FW
Network	FireWall	Barracuda	VPN
Network	FireWall	Check Point	SOHO
Network	FireWall	Check Point	Checkpoint Firewall
Network	FireWall	Cisco	Meraki_FW
Network	FireWall	Cisco	Cisco VPN Concentrator
Network	FireWall	Cisco	ASA_PIX_FW
Network	FireWall	Clavister	VS
Network	FireWall	CloudCover	Barrier1
Network	FireWall	Forcepoint	Firewall
Network	FireWall	Fortinet	FortiGate FW
Network	FireWall	Hewlett Packard	HPFireWall
Network	FireWall	Microsoft	Internet Security and Acceleration Server
Network	FireWall	Juniper Networks	SSL VPN

Network	FireWall	Juniper Networks	JunOS
Network	FireWall	Netmotion	Mobility_VPN
Network	FireWall	Netscreen	Netscreen Firewall
Network	FireWall	Palo Alto Networks	Firewall
Network	FireWall	Arbor Networks	PeakflowSP
Network	FireWall	pfSense	SG Firewall
Network	FireWall	Secure Computing	SecureComputing Firewall
Network	FireWall	Sonicwall	Sonicwall Firewall
Network	FireWall	Sophos	Firewall
Network	FireWall	VMware	NSX
Network	FireWall	WatchGuard Technologies	Firebox
Network	FireWall	Zscaler	Nanolog
Network	Network Access Control	Armis	NAC
Network	Network Access Control	Enterasys	Enter_NAC
Network	Network Access Control	ForeScout	CounterACT
Network	Network Access Control	Trustwave	Mirage NAC
Network	NetFlow	Cisco	Cisco_Netflow
Network	NetFlow	VCloud	VPC_Netflow
Network	NetFlow	NETFLOW	NETFLOW
Network	NetFlow	AWS	VPC_Netflow
Network	NetFlow	Microsoft	Azure_NSG_Flow_Logs
Network	Network Detection and Response	Cisco	Cisco NIDS
Network	Network Detection and Response	CloudCover	Barrier1
Network	Network Detection and Response	DarkTrace	DCIP
Network	Network Detection and Response	DB Networks	DBN6300
Network	Network Detection and Response	Fortinet	Fortinet IPS
Network	Network Detection and Response	Fortinet	Fortinet IPS

Network	Network Detection and Response	Fortinet	Fortinet IPS
Network	Network Detection and Response	IBM	PROVENTIA
Network	Network Detection and Response	McAfee	Network IPS
Network	Network Detection and Response	Security Onion	SecOnion_IPS
Network	Network Detection and Response	Snort	SNORT IDs
Network	Network Detection and Response	Sourcefire	Sourcefire Intrusion Sensor
Network	Network Detection and Response	Tanium	Threat Response
Network	Network Detection and Response	TippingPoint	UnityOne
SaaS	O365	Microsoft	Office 365
SaaS	O365	Microsoft	Office365_Advance_Threat_Protection_(ATP)
SaaS	O365	Microsoft	Office365_Audit_events
SaaS	O365	Microsoft	Office365_Azure_AD
SaaS	O365	Microsoft	Office365_Azure_AD_Identity_Protection
SaaS	O365	Microsoft	Office365_DLP
SaaS	O365	Microsoft	Office365_Exchange
SaaS	O365	Microsoft	Office365_Graph_Security_API
SaaS	O365	Microsoft	Office365_Microsoft_Cloud_App_Security_(MCAS)
SaaS	O365	Microsoft	Office365_Microsoft_Teams
SaaS	O365	Microsoft	Office365_Share_Point
SaaS	O365	Microsoft	Office365_Sway
SaaS	O365	Microsoft	Office365_Threat_Detection
SaaS	O365	Microsoft	Office365_Yammer
Web Application Firewall	Web Application Firewall	Breach WAF	Breach WAF
Web Application Firewall	Web Application Firewall	Cloudflare	Cloudflare_WAF
Web Application Firewall	Web Application Firewall	F5 Networks	ASM
Web Application Firewall	Web Application Firewall	Imperva	SecureSphere WAF

Web Application Firewall	Web Application Firewall	ModSecurity	ModSecurity Firewall
Web Application Firewall	Web Application Firewall	Trustwave	WAF