External Systems Support

FortiSOC 26.2.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 2, 2026
FortiSOC 26.2.1 External Systems Support
05-2621-1253773-20260602

Change log

Date	Change Description
2026-06-02	Initial release.

External systems support

The table below lists support for devices and applications (by vendor) configured in the *SIEM* module of FortiSOC version 26.2.1.

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
AirTight Networks	SpectraGuard	Discovered via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 125 event types parsed covering various Wireless suspicious activities	Currently not natively supported
Akamai	Akamai Connected Cloud				
Alcatel	TiMOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported
Alcatel	AOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported
Alert Logic	Intrusion Detection and Prevention Systems (IPS)	Host name and Device type	Not supported		Not supported
Alert Logic	Iris API	Host name and Device type	Not supported		Not supported
Alcide.io	KAudit	Not natively supported	Not natively supported	Kubernetes Audit logs	Not natively supported
Amazon	AWS Servers	AWS API: Server Name, Access	CloudWatch API: System Metrics: CPU, Disk I/O, Network	CloudTrail API: Over 325 event types parsed covering	CloudTrail API:

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		IP, Instance ID, Image Type, Availability Zone		various AWS activities	various administrative changes on AWS systems and users
Amazon	AWS Elastic Block Storage (EBS)	CloudWatch API: Volume ID, Status, Attach Time	CloudWatch API: Read/Write Bytes, Ops, Disk Queue		
Amazon	AWS EC2				
Amazon	AWS Elastic Load Balancer (ELB)				
Amazon	AWS Kinesis				
Amazon	AWS Relational Database Storage (RDS)		CloudWatch API: CPU, Connections, Memory, Swap, Read/Write Latency and Ops		
Amazon	Security Hub				
Amazon	Simple Queue Service				
Amazon	AWS S3 (Simple Storage Service)				
Apache	Tomcat Application Server	JMX: Version	JMX: CPU, memory, servlet, session, database, threadpool, request processor metrics	Currently not natively supported - Custom parsing needed	Currently not natively supported
Apache	Apache Web server	SNMP: Process name	SNMP: process level cpu, memory HTTPS via the mod-status module:	Syslog: W3C formatted access logs - per HTTP(S)	Currently not natively

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
			Apache level metrics	connection: Sent Bytes, Received Bytes, Connection Duration	supported
APC	NetBotz Environmental Monitor	SNMP: Host name, Hardware model, Network interfaces	SNMP: Temperature, Relative Humidity, Airflow, Dew point, Current, Door switch sensor etc.	SNMP Trap: Over 125 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported
APC	UPS	SNMP: Host name, Hardware model, Network interfaces	SNMP: UPS metrics	SNMP Trap: Over 49 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported
Apple	MacOS Servers and Workstations				
Arista Networks	Routers and Switches	SNMP: OS, Hardwar; SSH: configuration, running processes	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog and NetFlow	SSH: Running config, Startup config
Armis	Armis Asset Intelligence Platform				
Aruba Networks	CX Switching Platform			Syslog: Audit logs, General Performance and Availability logs	
Aruba Networks	Aruba Wireless LAN	SNMP: Controller OS, hardware,	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status SNMP: Access Point Wireless	SNMP Trap: Over 165 event types covering Authentication, Association,	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		Access Points	Channel utilization, noise metrics, user count	Rogue detection, Wireless IPS events	
Atlassian	Beacon				
Atlassian	Bitbucket				
Avaya	Call Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	CDR: Call Records	Currently not natively supported
Avaya	Session Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		Currently not natively supported
Barracuda Networks	Spam Firewall	Application type discovery via LOG	Currently not natively supported	Syslog: Over 20 event types covering mail scanning and filtering activity	Currently not natively supported
Barracuda Networks	Web Application Firewall			Syslog: System logs, Web Firewall logs, Access logs, Audit logs and Network Firewall logs	
Bit9	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported
Bitdefender				Syslog	
Blue Coat	Security Gateway Versions v4.x and later	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Proxy performance metrics	Syslog: Admin access to Security Gateway ; SFTP: Proxy traffic analysis	Currently not natively supported
Box.com	Cloud Storage	Currently not natively	Currently not natively supported	Box.com API: File creation, deletion, modify, file sharing	Currently not natively

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		supported			supported
Brocade	SAN Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Currently not natively supported	Currently not natively supported
Brocade	ServerIron ADX switch	SNMP: Host name, serial number, hardware	SNMP: Uptime, CPU, Memory, Interface Utilization, Hardware status, Real Server Statistics		
Carbon Black	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported
CentOS / Other Linux distributions	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports SSH: Hardware details, Linux distribution	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification; SSH: File integrity monitoring, Command output monitoring, Target file monitoring; FortiSIEM LinuxFileMon Agent: File integrity monitoring	SSH: File integrity monitoring, Target file monitoring; Agent: File integrity monitoring
CentOS / Other Linux distributions	DHCP Server	Currently not natively supported	Currently not natively supported	Syslog: DHCP activity (Discover, Offer, Request, Release etc) - Used in Identity and Location	Not Applicable
Checkpoint	FireWall-1 versions NG, FP1, FP2, FP3, AI	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log,	LEA: Firewall Audit trail

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	R54, AI R55, R65, R70, R77, NGX,R75, R80			Audit trail, over 940 IPS Signatures	
Checkpoint	GAIA	Host name and Device type		Over 9 event types	
Checkpoint	Provider-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	Currently not natively supported	Currently not natively supported	LEA: Firewall Log, Audit trail	LEA: Firewall Audit trail
Checkpoint	VSX	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail	LEA: Firewall Audit trail
Citrix	NetScaler Application Delivery Controller	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status, Application Firewall metrics	Syslog: Over 465 event types covering admin activity, application firewall events, health events	Currently not natively supported
Citrix	ICA	SNMP: Process Utilization	SNMP: Process Utilization; WMI: ICA Session metrics	Currently not natively supported	Currently not natively supported
Cisco	ASA Firewall (single and multi-context) version 7.x and later	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	SSH: Running config, Startup config

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Cisco	AMP				
Cisco	FireAMP				
Cisco	ASA firepower SFR Module	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	SSH: Running config, Startup config
Cisco	Firepower Threat Defense				
Cisco	CatOS based Switches	SNMP: OS, Hardware (Serial Number, Image file, Interfaces, Components); SSH: configuration running process	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config
Cisco	Duo		Not natively supported - Custom Monitoring needed	Via API	Not natively supported - Custom Custom Configuration collection needed
Cisco	PIX Firewall	SNMP: OS,	SNMP: CPU, Memory, Interface	Syslog: Over 1600 event	SSH: Running

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		Hardware SSH: interface security level needed for parsing traffic logs, Configuration	utilization, Connections, Hardware Status	types parsed for situations covering admin access, configuration change, traffic log, IPS activity	config, Startup config
Cisco	FWSM	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity	SSH: Running config, Startup config
Cisco	Identity Services Engine (ISE)	Host name and Device type			
Cisco	IOS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration, running process, Layer 2 connectivity	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics; SNMP: BGP metrics, OSPF metrics; SNMP: Class based QoS metrics; SNMP: NBAR metrics	Syslog: Over 200 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity; NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config
Cisco	Nexus OS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration running process, Layer 2	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics, BGP metrics, OSPF metrics, NBAR metrics; SNMP: Class based QoS metrics	Syslog: Over 3500 event types parsed for situations covering admin access, configuration change,	SSH: Running config, Startup config

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		connectivity		interface up/down, BGP interface up/down, traffic log, hardware status, software and hardware errors; NetFlow V5, V9: Traffic logs	
Cisco	ONS	SNMP: OS, Hardware		SNMP Trap: Availability and Performance Alerts	
Cisco	ACE Application Firewall	SNMP: OS, Hardware			
Cisco	UCS Server	UCS API: Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	UCS API: Chassis Status, Memory Status, Processor Status, Power Supply status, Fan status	Syslog: Over 500 event types parsed for situations covering hardware errors, internal software errors etc	Currently not natively supported
Cisco	WLAN Controller and Access Points	SNMP: OS, Hardware, Access Points	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status; SNMP: Access Point Wireless Channel utilization, noise metrics, user count	SNMP Trap: Over 88 event types parsed for situations covering Authentication, Association, Rogue detection, Wireless IPS events	Currently not natively supported
Cisco	Call Manager	SNMP: OS, Hardware, VoIP Phones	SNMP: Call manager CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource	Syslog: Over 950 messages from Cisco Call Manager as well as Cisco Unified Real	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
			usage; SNMP: VoIP phone count, Gateway count, Media Device count, Voice mail server count and SIP Trunks count; SNMP: SIP Trunk Info, Gateway Status Info, H323 Device Info, Voice Mail Device Info, Media Device Info, Computer Telephony Integration (CTI) Device Info	Time Monitoring Tool (RTMT); CDR Records, CMR Records: Call Source and Destination, Time, Call Quality metrics (MOS Score, Jitter, latency)	
Cisco	Contact Center	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Presence Server	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Tandberg Tele-presence Video Communication Server (VCS)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Tandberg Tele-presence Multiple Control Unit (MCU)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Unity Connection	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Cisco	IronPort Email Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Syslog: Over 45 event types covering mail scanning and forwarding status	Currently not natively supported
Cisco	IronPort Web Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	W3C Access log (Syslog): Over 9 event types covering web request handling status	Currently not natively supported
Cisco	Cisco Network IPS Appliances	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status	SDEE: Over 8000 IPS signatures	Currently not natively supported
Cisco	Sourcefire 3D and Defense Center	SNMP: OS, Hardware			
Cisco	Cisco Firepower Management Center (FMC) - Previously FireSIGHT Console			eStreamer SDK: Intrusion events, Malware events, File events, Discovery events, User activity events, Impact flag events	
Cisco	Cisco Security Agent	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	SNMP Trap: Over 25 event types covering Host IPS behavioral signatures.	Currently not natively supported
Cisco	Cisco Access Control Server (ACS)	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	Syslog: Passed and Failed authentications, Admin accesses	Currently not natively supported
Cisco	VPN 3000	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Syslog: Successful and Failed Admin Authentication, VPN Authentication, IPSec Phase 1 and Phase 2	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
				association, VPN statistics	
Cisco	Meraki Cloud Controllers	SNMP: OS, Hardware, Meraki devices reporting to the Cloud Controller	SNMP: Uptime, Network Interface Utilization; SNMP Trap: Various availability scenarios	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Meraki Firewalls	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization	Syslog: Firewall log analysis	Currently not natively supported
Cisco	Meraki Routers/Switches	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported
Cisco	Meraki WLAN Access Points	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported
Cisco	MDS Storage Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	Currently not natively supported - Custom parsing needed	Currently not natively supported
Cisco	Network Control Manager (NCM)			Syslog: Network device software update, configuration analysis for compliance, admin login	
Cisco	Stealthwatch	Host name and Device type	Not supported		Not supported
Cisco	Umbrella			DNS logs, Proxy logs, IP logs, Admin Audit logs	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Cisco	Viptela	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 289 Events Types parsed	Not natively supported - Custom configuration collection needed
Cisco	Wide Area Application Services (WAAS)	SNMP: Host name, Version, Hardware model, Network interfaces	SNMP: CPU, Memory, Interface utilization, Disk utilization, Process cpu/memory utilization		
Claroty	Continuous Threat Detection (CTD)				
Cloudflare	Cloudflare				
Cloud Native Computing Foundation (CNCF)	Kubernetes				
CloudPassage	Halo	Host name and Device type	Not supported		Not supported
Corero	Smartwall Threat Defense System				
CradlePoint	CradlePoint	Discovered via LOG only	Not natively supported. Custom monitoring needed	29 Event types covering Security Violations, Config Changes, Authentications and informational events	Not currently supported.
CrowdStrike	Falcon	Host name and	Not supported		Not supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		Device type			
Cybereason	Cybereason				
Cyberoam	Cyberoam	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Event, Security, and Traffic logs	Connection - permit and deny, system events, maleware events
Cylance	Cylance Protect Endpoint Protection			Syslog: Endpoint protection alerts	
Cyphort	Cyphort Cortex Endpoint Protection			Syslog: Endpoint protection alerts	
Cyxtera	AppGate SDP	Host name and Device type	Not supported		Not supported
Damballa	Failsafe				
Darktrace	CyberIntelligence Platform	Discovered via LOG only	Not natively supported - Custom monitoring needed	Over 40 Events Types parsed	Not Natively Supported - Custom Configuration collection needed
Dell	SonicWall Firewall	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Firewall session count	Syslog: Firewall log analysis (over 1000 event types)	Currently not natively supported
Dell	Force10 Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Interface Status, Hardware Status		SSH: Running config, Startup config

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Dell	NSeries Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config
Dell	PowerConnect Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config
Dell	Dell Hardware on Intel-based Servers	SNMP: Hardware	SNMP: Hardware Status: Battery, Disk, Memory, Power supply, Temperature, Fan, Amperage, Voltage		Currently not natively supported.
Dell	Compellent Storage	SNMP: OS, Hardware	SNMP: Network Interface utilization, Volume utilization, Hardware Status (Power, Temperature, Fan)		Currently not natively supported.
Dell	EqualLogic Storage	SNMP: OS, Hardware (Network interfaces, Physical Disks, Components)	SNMP: Uptime, Network Interface utilization; SNMP: Hardware status: Disk, Power supply, Temperature, Fan, RAID health; SNMP: Overall Disk health metrics: Total disk count, Active disk count, Failed disk count, Spare disk count; SNMP: Connection metrics: IOPS, Throughput; SNMP: Disk performance metrics: IOPS, Throughput; SNMP: Group level performance metrics: Storage, Snapshot		Currently not natively supported.
Digital Defense	Frontline Vulnerability Manager			Frontline API: Host name, Vulnerability name, Vulnerability CVE ID, Vulnerability score, and operating system in event.	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Digital Guardian	Code Green DLP	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported
Dragos	Platform - Industrial control systems (ICS) and OT (operational technology)				
Dynatrace	Dynatrace				
EMC	Clariion Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces, Installed Software, Storage Controller Ports; Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization		Currently not natively supported.

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		mappings, Storage Groups and memberships			
EMC	VNX Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces, Installed Software, Storage Controller Ports Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group mappings, Storage Groups and memberships	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization		
EMC	Isilon Storage	SNMP: Host	SNMP: Uptime, Network Interface	5 event types	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks, Components)	metrics; SNMP: Hardware component health: Disk, Power supply, Temperature, Fan, Voltage; SNMP: Cluster membership change, Node health and performance (CPU, I/O), Cluster health and performance, Cluster Snapshot, Storage Quota metrics, Disk performance, Protocol performance		
Epic	SecuritySIEM	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication Query, Client login Query	Currently not natively supported
ESET	Nod32 Anti-virus	Application type discovery via LOG		Syslog (CEF format): Virus found/cleaned type of events	
FireEye	Malware Protection System (MPS)	Application type discovery via LOG		Syslog (CEF format): Malware found/cleaned type of events	
FireEye	HX Appliances for Endpoint protection	Application type discovery via LOG		Syslog (CEF format): Malware Acquisition, Containment type of events	
F5 Networks	Application Security Manager	Discovery via LOG		Syslog (CEF Format); Various application level attack scenarios - invalid directory access, SQL injections, cross site exploits	
F5 Networks	Local Traffic	SNMP: Host	SNMP: CPU, Memory, Disk, Interface	SNMP Trap: Exception	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	Manager	name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks), Installed Software, Running Software	utilization, Process monitoring, Process stop/start	situations including hardware failures, certain security attacks, Policy violations etc; Syslog: Permitted and Denied Traffic	
F5 Networks	Web Accelerator	Discovery via LOG		Syslog: Permitted Traffic	
Fortinet	FortiNDR (Formerly FortiAI)				
Fortinet	FortiNDR Cloud				
Fortinet	FortiAnalyzer				
Fortinet	FortiAP	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Wireless events via FortiGate	
Fortinet	FortiAuthenticator	Vendor, OS, Model	Interface Stat, Authentication Stat	Over 150 event types	Currently not natively supported.

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Fortinet	FortiCASB				
Fortinet	FortiClient	Discovered via LOG only		Syslog: Traffic logs, Event logs	Not supported
Fortinet	FortiClient EMS				
Fortinet	FortiDeceptor	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication logs, Decoy activity	Currently not natively supported.
Fortinet	FortiEDR	Discovered via LOG only	Not natively supported. Custom monitoring needed.	System and security events (e.g. file blocked)	Currently not natively supported
Fortinet	FortiGate firewalls	SNMP: OS, Host name, Hardware (Serial Number, Interfaces, Components)	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics	Syslog: Over 11000 Traffic and system logs; Netflow: traffic flow, Application flow	SSH: Running config, Startup config
Fortinet	FortiManager	SNMP: Host name, Hardware model, Network interfaces, Operating system version	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics		
Fortinet	FortiMail Workspace Security				
Fortinet	FortiNAC	Discovered via LOG only	Not natively supported. Custom monitoring needed	Administrative and User Admission Control events	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Fortinet	FortiPAM / FortiSRA				
Fortinet	FortiProxy				
Fortinet	FortiRecon				
Fortinet	FortiTester	Discovered Via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 14 Event types parsed	Not natively supported - Custom configuration collection needed
Fortinet	FortiWLC	SNMP - Controller – Name, OS, Serial Number, Interfaces, Associated Access Points – name, OS, Interfaces	Controller – CPU, Memory, Disk, Throughput, QoS statistics, Station count	Hardware/Software errors, failures, logons, license expiry, Access Point Association / Disassociation	Not supported
Foundry Networks	IronWare Router and Switch	SNMP: OS, Hardware SSH: configuration, running process	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 6000 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config
FreeBSD					
G42 Cloud	G42 Cloud				
GitHub.com	GitHub	Host name and Device type	Not supported		Not supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
GitLab	GitLab				
GitLab API	GitLab	Host name and Device type	Not supported		Not supported
GitLab CLI	GitLab	Host name and Device type	Not supported		Not supported
Google	Google Cloud Platform				
Google	Google Workspace (Formerly G Suite and Google Apps)				
Green League	WVSS				
Hillstone Networks	Hiistone Firewall				
Hirschmann	Switches	Host Name, OS	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Not natively supported - Custom parsing needed	Not natively supported - Custom configuration collection needed
HP	BladeSystem	SNMP: Host name, Access IP, Hardware components	SNMP: hardware status		
HP	HP-UX servers	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Disk space utilization, Network Interface Errors,		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
			Running Process Count, Running process CPU/memory utilization, Running process start/stop; SNMP: Installed Software change; SSH : Memory paging rate, Disk I/O utilization		
HP	HP Hardware on Intel-based Servers	SNMP: hardware model, hardware serial, hardware components (fan, power supply, battery, raid, disk, memory)	SNMP: hardware status	SNMP Trap: Over 100 traps covering hardware issues	
HP	TippingPoint UnityOne IPS	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors	Syslog: Over 4900 IPS alerts directly or via NMS	
HP	ProCurve Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status		SSH: Running config, Startup config
HP	Value Series (19xx) Switches and Routers	SNMP: OS, hardware	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		model, hardware serial, hardware components; SSH: configuration			
HP	3Com (29xx) Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config
HP	HP/3Com Comware Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status	Syslog: Over 6000 vent types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup config
HPE	Aruba Networking ClearPass Policy Manager				
HPE	Integrated Lights-Out (iLO)				
Huawei	VRP Router and Switch	SNMP: OS, Hardware; SSH:	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware	Syslog: Over 30 event types parsed for situations	SSH: Running config, Startup

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		configuration, running process, Layer 2 connectivity	Status	covering admin access, configuration change, interface up/down	config
HyTrust	CloudControl	LOG Discovery	Currently not natively supported	Over 70 event types	Currently not natively supported
IBM	Websphere Application Server	SNMP or WMI: Running processes	HTTP(S): Generic Information, Availability metrics, CPU / Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics		
IBM	DB2 Database Server	SNMP or WMI: Running processes	JDBC: Database Audit trail: Log on, Database level and Table level CREATE/DELETE/MODIFY operations		
IBM	ISS Proventia IPS Appliances			SNMP Trap: IPS Alerts: Over 3500 event types	
IBM	AIX Servers	SNMP: OS, Hardware, Installed Software, Running Processes, Open Ports; SSH: Hardware details	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
IBM	OS 400			Syslog via PowerTech Agent: Over 560 event types	
Imperva	Securesphere DB Monitoring Gateway				
Imperva	Securesphere Security Gateway			Syslog in CEF format	
Imperva	Securesphere Web App Firewall				
Infoblox	DNS/DHCP Appliance	SNMP: OS, Hardware, Installed Software, Running Processes	; SNMP: Zone transfer metrics, DNS Cluster Replication metrics, DNS Performance metrics, DHCP Performance metrics, DDNS Update metrics, DHCP subnet usage metrics ; SNMP: Hardware Status ; SNMP Trap: Hardware/Software Errors	Syslog: DNS logs - name resolution activity - success and failures	
ISC	Bind DNS			Syslog: DNS logs - name resolution activity - success and failures	
Juniper	JunOS Router/Switch	SNMP: OS, Hardware; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status ;	Syslog: Over 1420 event types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration
Juniper	SRX Firewalls	SNMP: OS, Hardware SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering traffic log, admin	SSH: Startup configuration

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
				access, configuration change, interface up/down and other hardware issues and internal errors	
Juniper	SSG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration
Juniper	ISG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration
Juniper	Steel-belted Radius	Discovered via LOG		Syslog - 4 event types covering admin access and AAA authentication	
Juniper	Secure Access Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk, Interface utilization	Syslog - Over 30 event types parsed for situations covering VPN login, Admin access, Configuration Change	
Juniper	Netscreen IDP			Syslog - directly from Firewall or via NSM - Over 5500 IPS Alert types parsed	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Juniper	DDoS Secure			Syslog - DDoS Alerts	
Kaspersky				Syslog	
KVM					
Lantronix	SLC Console Manager			Syslog - Admin access, Updates, Commands run	
LastLine				Syslog in CEF format	
Liebert	HVAC	SNMP: Host Name, Hardware model	SNMP: HVAC metrics: Temperature: current value, upper threshold, lower threshold, Relative Humidity: current value, upper threshold, lower threshold, System state etc		
Liebert	FPC	SNMP: Host Name, Hardware model	SNMP: Output voltage (X-N, Y-N, Z-N), Output current (X, Y. Z), Neutral Current, Ground current, Output power, Power Factor etc		
Liebert	UPS	SNMP: Host Name, Hardware model	SNMP: UPS metrics: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage etc		
Malwarebytes	Malwarebytes Breach Remediation				
Malwarebytes	Malwarebytes Endpoint Protection				
ManageEngine	Endpoint Central				
ManageEngine	PAM360				

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
McAfee	ePolicy Orchestrator (ePO)	SNMP: Related process name and parameters	SNMP: Process resource utilization	SNMP Trap: Over 170 event types	
McAfee	Network Security Platform	SNMP: OS, Hardware	SNMP: Hardware status	Syslog: IPS Alerts	
McAfee	Stonesoft Intrusion Prevention System (IPS)			Syslog: IPS Alerts	
McAfee	McAfee Web Gateway			Syslog: Web server log	
Microsoft	ASP.NET	SNMP: Running Processes	SNMP or WMI: Process level resource usage ; WMI: Request Execution Time, Request Wait Time, Current Requests, Disconnected Requests etc		
Microsoft	Microsoft Advanced Threat Analytics (ATA) On Premise Platform				
Microsoft	Microsoft Defender for Endpoint	Host name and Device type	Not supported		Not supported
Microsoft	Azure Compute				
Microsoft	Azure Event Hub				
Microsoft	Cloud App Security	Host name and Device type	Not supported		Not supported
Microsoft	DHCP Server - 2003,	SNMP: Running	WMI: DHCP metrics: request rate,	FortiSIEM Windows Agent	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	2008	Processes	release rate, decline rate, Duplicate Drop rate etc	(HTTPS): DHCP logs - release, renew etc; Snare Agent (syslog): DHCP logs - release, renew etc; Correlog Agent (syslog): DHCP logs - release, renew etc	
Microsoft	DNS Server - 2003, 2008	SNMP: Running Processes	WMI: DNS metrics: Requests received, Responses sent, WINS requests received, WINS responses sent, Recursive DNS queries received etc	FortiSIEM Windows Agent (HTTPS): DNS logs - name resolution activity; Snare Agent (syslog): DNS logs - name resolution activity; Correlog Agent (syslog): DNS logs - name resolution activity	
Microsoft	Domain Controller / Active Directory - 2003, 2008, 2012	SNMP: Running Processes; LDAP: Users	WMI: Active Directory metrics: Directory Search Rate, Read Rate, Write Rate, Browse Rate, LDAP search rate, LDAP Bind Rate etc; WMI: "dcdiag -e" command output - detect successful and failed domain controller diagnostic tests; WMI: "repadmin /replsummary" command output - Replication statistics; LDAP: Users with stale passwords, insecure password settings		
Microsoft	Entra Identity Protection				
Microsoft	Exchange Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage; WMI: Exchange		Exchange Tracker Logs via FSM Advanced

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
			performance metrics, Exchange error metrics, Exchange mailbox metrics, Exchange SMTP metrics, Exchange ESE Database, Exchange Database Instances, Exchange Mail Submission Metrics, Exchange Store Interface Metrics etc		Windows Agent
Microsoft	Hyper-V Hypervisor		Powershell over winexe: Guest/Host CPU usage, Memory usage, Page fault, Disk Latency, Network usage ;		
Microsoft	IIS versions	SNMP: Running Processes	SNMP or WMI: Process level resource usage WMI: IIS metrics: Current Connections, Max Connections, Sent Files, Received Files etc	FortiSIEM Windows Agent (HTTPS): W3C Access logs - Per instance Per Connection - Sent Bytes, Received Bytes, Duration ; Snare Agent (syslog): W3C Access logs; Correlog Agent (syslog): W3C Access logs	
Microsoft	Internet Authentication Server (IAS)	SNMP: Running Processes	SNMP or WMI: Process level resource usage	FortiSIEM Windows Agent (HTTPS): AAA logs - successful and failed authentication ; Snare Agent (syslog): AAA logs - successful and failed authentication ; Correlog Agent (syslog): AAA logs - successful and failed authentication	
Microsoft	Network Policy Server	Discovered via LOG only.	Not natively supported. Custom monitoring needed.	AAA-based login events	Currently not natively

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
					supported
Microsoft	PPTP VPN Gateway			FortiSIEM Windows Agent (HTTPS): VPN Access - successful and failed Snare Agent (syslog): VPN Access - successful and failed ; Correlog Agent (syslog): VPN Access - successful and failed	
Microsoft	SharePoint Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage	LOGBinder Agent: SharePoint logs - Audit trail integrity, Access control changes, Document updates, List updates, Container object updates, Object changes, Object Import/Exports, Document views, Information Management Policy changes etc	
Microsoft	SQL Server - 2014, 2016, 2017, 2019	SNMP: Running Processes	SNMP or WMI: Process resource usage; JDBC: General database info, Configuration Info, Backup Info,; JDBC: Per-instance like Buffer cache hit ratio, Log cache hit ratio etc; JDBC: per-instance, per-database Performance metrics Data file size, Log file used, Log growths etc; JDBC: Locking info, Blocking info	JDBC: database error log; JDBC: Database audit trail	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Microsoft	Microsoft Defender for Endpoint/Windows Defender Advanced Threat Protection (ATP)	Host name and Device type	Not supported		Not supported
Microsoft	Windows 2000, Windows 2003, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2	SNMP: OS, Hardware (for Dell and HP), Installed Software, Running Processes; WMI: OS, Hardware (for Dell and HP), BIOS, Installed Software, Running Processes, Services, Installed Patches	SNMP: CPU, Memory, Disk, Interface utilization, Process utilization ; WMI: SNMP: CPU, Memory, Disk, Interface utilization, Detailed CPU/Memory usage, Detailed Process utilization	WMI pulling: Security, System and Application logs; FortiSIEM Windows Agent (HTTPS): Security, System and Application logs, File Content change; Snare Agent (syslog): Security, System and Application logs; Correlog Agent (syslog): Security, System and Application logs	SNMP: Installed Software Change; FortiSIEM Windows Agent: Installed Software Change, Registry Change; FortiSIEM Windows Agent: File Integrity Monitoring
Mimecast	Mimecast Cloud Gateway				
MobileIron Sentry and Connector	Sentry	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 18 Events Types parsed	Not natively supported - Custom configuration collection

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
					needed
Motorola	AirDefense Wireless IDS			Syslog: Wireless IDS logs	
Motorola	WiNG WLAN Access Point			Syslog: All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	
Mikrotek	Mikrotech Switches and Routers	Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU utilization, Network Interface metrics		
NetApp	DataONTAP				
NetApp	DataONTAP based Filers	SNMP: Host name, OS, Hardware model, Serial number, Network interfaces, Logical volumes, Physical Disks	SNMP: CPU utilization, Network Interface metrics, Logical Disk Volume utilization; SNMP: Hardware component health, Disk health ONTAP API: Detailed NFS V3/V4, ISCSI, FCP storage IO metrics, Detailed LUN metrics, Aggregate metrics, Volume metrics, Disk performance metrics	SNMP Trap: Over 150 alerts - hardware and software alerts	
Nessus	Vulnerability Scanner			Nessus API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity,	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
				Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence, etc	
Netwrix	Auditor	Not natively supported	Not natively supported	2 Event Types parsed (via Windows Correlog Agent)	Not natively supported
NGINX	Web Server	SNMP: Application name	SNMP: Application Resource Usage	Syslog: W3C access logs: per HTTP(S) connection: Sent Bytes, Received Bytes, Connection Duration	
Nimble	NimbleOS Storage	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime, Network Interface metrics, Storage Disk Utilization SNMP: Storage Performance metrics: Read rate (IOPS), Sequential Read Rate (IOPS), Write rate (IOPS), Sequential Write Rate (IOPS), Read latency, etc		
Nortel	ERS Switches and Routers	SNMP: Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status		
Nortel	Passport Switches and Routers	SNMP: Host name, OS, Hardware	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		model, Serial number, Components			
Nozomi	Central Management Control (CMC)				
Nozomi	Guardian	No	No	Yes	No
Nutanix	Controller VM	SNMP: Host name, OS, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Disk Status, Cluster Status, Service Status, Storage Pool Info, Container Info		
Nutanix	Nutanix Prism			API Audit, Audit, Security Policy Hitlogs, and Flow Service Logs	
Okta.com	SSO	Okta API: Users		Okta API: Over 90 event types covering user activity in Okta website	
One Identity	Safeguard		Not supported		
OpenLDAP	OpenLDAP	LDAP: Users			
Oracle	Cloud Access Security Broker (CASB)				

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Oracle	Cloud Infrastructure				
Oracle	Enterprise Database Server - 10g, 11g, 12c, 18/19c, 21c	SNMP or WMI: Process resource usage ;	JDBC: Database performance metrics: Buffer cache hit ratio, Row cache hit ratio, Library cache hit ratio, Shared pool free ratio, Wait time ratio, Memory Sorts ratio etc ; JDBC: Database Table space information: able space name, table space type, table space usage, table space free space, table space next extent etc; JDBC: Database audit trail: Database logon, Database operations including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc.	Syslog: Listener log, Alert log, Audit Log	
Oracle	MySQL Server	SNMP or WMI: Process resource usage	JDBC: User Connections, Table Updates, table Selects, Table Inserts, Table Deletes, Temp Table Creates, Slow Queries etc; JDBC: Table space performance metrics: Table space name, table space type, Character set and Collation, table space usage, table space free space etc; JDBC: Database audit trail: Database log on, Database/Table CREATE/DELETE/MODIFY operations		
Oracle	WebLogic	SNMP or WMI:	JMX: Availability metrics, Memory		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	Application Server	Process resource usage	metrics, Servlet metrics, Database metrics, Thread pool metrics, EJB metrics, Application level metrics		
Oracle	Glassfish Application Server	SNMP or WMI: Process resource usage	JMX: Availability metrics, Memory metrics, Servlet metrics, Session metrics, Database metrics, Request processor metrics, Thread pool metrics, EJB metrics, Application level metrics, Connection metrics		
Oracle	Sun SunOS and Solaris	SNMP: OS, Hardware, Software, Processes, Open Ports ; SSH: Hardware details	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification	
OTORIO	RAM2 (Risk Assessment, Monitoring and Management)				
PacketFence	Network Access Control	Host name and Device type	Not supported		Not supported
Palo Alto Networks	Palo Alto Cortex XDR				
Palo Alto Networks	Palo Alto Traps Endpoint Security Manager	LOG Discovery	Currently not natively supported	Over 80 event types	Currently not natively supported
Palo Alto	PAN-OS based	SNMP: Host	SNMP: Uptime, CPU utilization,	Syslog: Traffic log, Threat	SSH:

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Networks	Firewall	name, OS, Hardware, Network interfaces; SSH: Configuration	Network Interface metrics, Firewall connection count	log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs, wildfire logs	Configuration Change
Pathlock	Identity Security Platform				
Proofpoint	Proofpoint				
PulseSecure	PulseSecure VPN			Syslog: VPN events, Traffic events, Admin events	
QNAP	Turbo NAS				
Qualys	QualysGuard Scanner				
Qualys	Vulnerability Scanner			Qualys API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc	
Qualys	Web Application Firewall			syslog (JSON formatted): web log analysis	
Radware	DefensePro	LOG Discovery	Currently not natively supported	Over 120 event types	Currently not natively supported

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
Rapid7	InsightVM (Platform Based Vulnerability Management)	Host name and Device type	Not supported		
Rapid7	NeXpose Vulnerability Scanner (Vulnerability Management On-Premises)			Rapid7 NeXpose API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc	
Red Hat	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports ; SSH: Hardware details, Linux distribution	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification SSH: File integrity monitoring, Command output monitoring, Target file monitoring Agent: File integrity monitoring	SSH: File integrity monitoring, Target file monitoring Agent: File integrity monitoring
Red Hat	JBoss Application Server	SNMP: Process level CPU/Memory usage	JMX: CPU metrics, Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics	;	
Red Hat	DHCP Server	SNMP: Process level		Syslog: DHCP address release/renew events	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
		CPU/Memory usage			
Riverbed	Steelhead WAN Accelerators	SNMP: Host name, Software version, Hardware model, Network interfaces	SNMP: Uptime, CPU / Memory / Network Interface / Disk space metrics, Process cpu/memory utilization; SNMP: Hardware Status SNMP: Bandwidth metrics: (Inbound/Outbound Optimized Bytes - LAN side, WAN side; Connection metrics: Optimized/Pass through / Half-open optimized connections etc); SNMP: Top Usage metrics: Top source, Top destination, Top Application, Top Talker; SNMP: Peer status: For every peer: State, Connection failures, Request timeouts, Max latency	SNMP Trap: About 115 event types covering software errors, hardware errors, admin login, performance issues - cpu, memory, peer latency issues ; Netflow: Connection statistics	
Ruckus	Wireless LAN	SNMP: Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	SNMP: Controller Uptime, Controller Network Interface metrics, Controller WLAN Statistics, Access Point Statistics, SSID performance Stats		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
SAP	SAP Enterprise Threat Detection (ETD)				
SAP	SAP Enterprise Threat Detection Cloud				
Security Onion	Zeek (Bro)	Discovered via LOG only	Not natively supported - Custom monitoring needed	Syslog JSON format: 6 event types parsed	Currently not natively supported
SentinelOne	SentinelOne Singularity				
Siemens	Simatic PLC				
Snort	IPS	SNMP: Process level CPU/Memory usage		Syslog: Over 40K IPS Alerts DBC: Over 40K IPS Alerts - additional details including TCP/UDP/ICMP header and payload in the attack packet	
SolarWinds	Orion	SNMP			
Sophos	Central	Host name and Device type	Not supported		Not supported
Sophos	Sophos Endpoint Security and Control			SNMP Trap: Endpoint events including Malware found/deleted, DLP events	
Squid	Web Proxy	SNMP: Process level CPU/Memory usage		Syslog: W3C formatted access logs - per HTTP(S) connection: Sent Bytes, Received Bytes, Connection	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
				Duration	
SSH Com Security	CryptoAuditor	LOG Discovery	Currently not natively supported	Many event types	Currently not natively supported
Stormshield	Network Security	Not natively supported	Not natively supported	Firewall logs	Not natively supported
Symantec	Symantec Endpoint Protection			Syslog: Over 5000 event types covering end point protection events - malware/spyware/adware, malicious events	
Tanium	Connect	Host name and Device type	Not supported		Not supported
Tenable	Tenable.io	Host name and Device type	Not supported		Not supported
Thales	Vormetric Data Security Manager	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported
Tigera	Calico	Not natively supported	Not natively supported	Flow, Audit and DNS logs	Not natively supported
Trellix	Sidewinder Firewall	SNMP: OS, Hardware, Installed Software, Running Processes	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	Syslog: Firewall logs	
Trellix	McAfee Vulnerability			JDBC: Vulnerability data	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	Manager				
Trend Micro	Deep Discovery	Discovered via LOG only	Not natively supportedCustom monitoring needed.	Malicious file detection	Currently not natively supported
Trend Micro	Deep Security Manager			Syslog: Over 10 event types covering end point protection events	Not supported
Trend Micro	Interscan Web Filter	LOG Discovery	Currently not natively supported	15 event Types	Currently not natively supported
Trend Micro	Intrusion Defense Firewall (IDF)			Syslog: Over 10 event types covering end point firewall events	
Trend Micro	Office scan			SNMP Trap: Over 30 event types covering end point protection events - malware/spyware/adware, malicious events	
Trend Micro	Trend Vision One				
Ubiquiti	Wireless LAN Controller				
UserGate	UTM Firewall				
Vasco	DigiPass			Syslog - Successful and Failed Authentications, Successful and Failed administrative logons	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
VMware	VMware ESX and VCenter	VMWare SDK: Entire VMware hierarchy and dependencies - Data Center, Resource Pool, Cluster, ESX and VMs	VMWare SDK: VM level: CPU, Memory, Disk, Network, VMware tool status VMWare SDK: ESX level: CPU, Memory, Disk, Network, Data store VMWare SDK: ESX level: Hardware Status VMWare SDK: Cluster level: CPU, Memory, Data store, Cluster Status VMWare SDK: Resource pool level: CPU, Memory	VMWare SDK: Over 800 VCenter events covering account creation, VM creation, DRS events, hardware/software errors	
VMware	NSX for vSphere				
VMware	vShield			Syslog: Over 10 events covering permitted and denied connections, detected attacks	
VMware	VCloud Network and Security (vCNS) Manager			Syslog: Over 10 events covering various activities	
WALLIX	Bastion				
WatchGuard	Firebox Firewall			Syslog: Over 20 firewall event types	
Websense	Web Filter			Syslog: Over 50 web filtering events and web traffic logs	
Workday	Workday Enterprise Suite				
YXLink	Vulnerability Scanner				
Zeek	Network Security				

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring
	Monitor (Previously known as Bro)				
Zscaler	Zscaler Internet Access (ZIA)				
Zscaler	Zscaler Private Access (ZPA)				

www.fortinet.com