11:11 SYSTEMS

11:11 MANAGED SIEM

DEVICES AND APPLICATIONS BY VENDOR

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

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
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 IP, Instance ID, Image Type, Availability Zone	CloudWatch API: System Metrics: CPU, Disk I/O, Network	CloudTrail API: Over 325 event types parsed covering various AWS activities	CloudTrail API: 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 Relational Database Storage (RDS)		CloudWatch API: CPU, Connections, Memory, Swap, Read/Write Latency and Ops		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Amazon	Security Hub				
Alcatel	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
Alcatel	Apache Web server	SNMP: Process name	SNMP: process level l spu, memory HTTPS via the mod-status module: Apache level metrics	Syslog: W3C formatted access logs - per HTTP (S) connection: Sent Bytes, Received Bytes, Connection Duration	Currently not natively 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
Arista Networks	Routers and Switches	SNMP: OS, Hardware: SSH: configuration, running processes	SNMP: CPU, memory, interface utilization, hardware status	Syslog and NetFlow	SSH: Running config, Startup config
Aruba Networks	Aruba Wireless LAN	SNMP: Controller 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 165 event types covering Authentication, Association Rogue detection, Wireless IPS events	Currently not natively supported
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	Spam Firewall	Application	Currently not natively supported	Syslog: Over 20 event	Currently not

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Networks		type discovery via LOG		types covering mail scanning and filtering activity	natively supported
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
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 supported	Currently not natively supported	Box.com API: File creation, deletion, modify, file sharing	Currently not natively 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
Cent OS / 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 (Discovery, Offer, Request, Release etc)- Used in Identity and Location	Not Applicable

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Checkpoint	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail, over 940 IPS Signatures	LEA: Firewall Audit trail
Checkpoint	GAIA	Host name and Device type		Over 9 event types	
Checkpoint	Provide-1 version 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
Cisco	AMP				
Cisco	FireAMP				
Cisco	ASA firepower SFR Module	SNMP: OS, Hardware SSH:	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin	SSH: Running config,

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		interface security level needed for parsing traffic logs, Configuration		access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	Startup config
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, 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	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

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Cisco	Identify 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 connectivity	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, interface up/down, BGP interface up/down, traffic log, hardware status, software and hardware errors; NetFlow V5, V9: Traffic logs	SSH: Running config. Startup config
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	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status; SNMP: Access Point	SNMP Trap: Over 88 event types parsed for situations covering	Currently not natively supported

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Points	Wireless Channel utilization, noise metrics, user count	Authentication, Association, Rogue detection, Wireless IPS events	
Cisco	Call Manager	SNMP: OS, Hardware, VoIP Phones	SNMP: Call manager CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource 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	Syslog: Over 950 messages from Cisco Call Manager as well as Cisco Unified Real Time Monitoring Tool (RTMT); CDR Records, CMR Records: Call Source and Destination, Time, Call Quality metrics (MOS Score, Jitter, latency)	Currently not natively supported
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	Tandeberg 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	Tandeberg 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
Cisco	IronPort Mail 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	W3C Access log	Currently not natively

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
			Interface utilization, Hardware Status, Process level resource usage, Install software change	(Syslog): Over 9 event types covering web request handling status	supported
Cisco	Cisco Network IPS Appliances	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status	SDEEL Over 8000 IPS signature	Currently not natively supported
Cisco	Sourcefire 3D and Defense Center	SNMP: OS, Hardware			
Cisco	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 signature.	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 association, VPN statistics	Currently not natively supported
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	SNMP: OS,	SNMP: Uptime, Network Interface		Currently not

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
	Routers/Switches	Hardware	Utilization		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	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)				
CloudPassage	Halo	Host name and Device type	Not supported		Not supported
Corero	Smartwall Threat Defense System				
CradlePoint	CradlePoint	Discovered	Not natively supported. Custom	29 Events types covering	Not currently

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		via LOG only	monitoring needed	Security Violations, Config Changes, Authentications and informational events	supported
CrowdStike	Falcon	Host name and Device type	Not supported		Not supported
Cyberoam	Cyberoam	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Event, Security, and Traffic logs	Connection - permit and deny, system events, malware 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
Dell	NSeries Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: config

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
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 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)				
EMC	Clarion Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number,	Naviseccli: Storage Processor utilization, Storage Port I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization		Currently not natively supported.

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		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			
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	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		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Groups and memberships			
EMC	Isilon Storage	SNMP: Host name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks, Components)	SNMP: Uptime, Network Interface 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 Quote metrics, Disk performance, Protocol performance	5 event types	
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 Manager	SNMP: Host name, Operating system, Hardware (Model, Serial number,	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	SNMP Trap: Exception situations including hardware failures, certain security attacks, Policy violations etc; Syslog: Permitted and Denied Traffic	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Network interfaces, Physical Disks), Installed Software, Running Software			
F5 Networks	Web Accelerator	Discovery via LOG		Syslog: Permitted Traffic	
Fortinet	FortiAnalyzer			Aggregated event data	
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 vent types	Currently not natively supported.
Fortinet	FortiClient	Discovered via LOG only		Syslog: Traffic logs, Event logs	Not supported
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	FortiInsight				
Fortinet	FortiManager	SNMP: Host name, Hardware model, Network	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		interfaces, Operating system version			
Fortinet	FortiNAC	Discovered via LOG only	Not natively supported. Custom monitoring needed	Administrative and User Admission Control events	Currently not natively supported
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
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
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					
GitHub.com	GitHub	Host name and Device type	Not supported		Not supported
GitLab API	GitLab	Host name and Device type	Not supported		Not supported
GitLab CLI	GitLab	Host name and Device type	Not supported		Not supported
Green League	WVSS				

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Huawei	VRP Router and Switch	SNMP: OS, Hardware, SSH: configuration, running process, Layer 2 connectivity	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 30 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config
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, Running Process Count, Running process CPU/memory utilization, Running process start/stop; SNMP: Install 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	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status		SSH: Running config, Startup

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		serial, hardware components; SSH: configuration			config
HP	Value Series (19xx) 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	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 event types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup config
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
HyTrust	CloudControl	LOG Discovery	Currently not natively supported	Over 70 event types	Currently not natively supported
IBM	Websphere	SNMP or	HTTP(S): Generic Information,		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
	Application Server	WMI: Running processes	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	
IBM	OS 400			Syslog via PowerTech Agent: Over 560 event types	
Imperva	Securesphere DB Monitoring Gateway				
Imperva	Securesphere DB Security Gateway			Syslog in CEF format	
Imperva	Securesphere Web App Firewall				
Indegy	Security Platform	Discovered via LOG only	Not natively supported - Custom monitoring needed	Over 14 Event Types parsed	Not natively supported - Custom configuration collection needed
Intel/McAfee	McAfee	SNMP: OS,	SNMP: CPU, Memory, Disk	Syslog: Firewall logs	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
	Sidewinder Firewall	Hardware, Installed Software, Running Processes	Interface utilization, Process monitoring, Process stop/start		
Intel/McAfee	McAfee ePO	Snmp: Related process name and parameters	SNMP: Process resource utilization	SNMP Trap: Over 170 event types	
Intel/McAfee	Intrushield IPS	SNMP: OS, Hardware	SNMP: Hardware status	Syslog: IPS Alerts	
Intel/McAfee	Intrushield IPS			Syslog: IPS Alerts	
Intel/McAfee	Web Gateway			Syslog: Web server log	
Intel/McAfee	Foundstone Vulnerability Scanner			JDBC: Vulnerability data	
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	
Intel/McAfee	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;	SNMP: CPU, Memory, Disk, Interface utilization, Hardware	Syslog: Over 1420 event types parsed for	SSH: Startup configuration

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		SSH: Configuration	Status	situations covering traffic log, admin 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	
Juniper	DDoS Secure			Syslog - DDoS Alerts	
Lantronix	SLC Console Manager			Syslog - Admin access, Updates, Commands run	
LastLine				Syslog in CEF format	
Liebert	HVAC	SNMP: Host Name, Hardware	SNMP: HVAC metrics: Temperature: current value, upper threshold, lower threshold, Relative		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		model	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 batter charge, Battery status, Time on battery, Estimated seconds Remaining, Output voltage etc		
Malware bytes	Malwarebytes Breach Remediation				
Malware bytes	Malwarebytes Endpoint Protection				
McAfee	Vormetric Data Security Manager	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported
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 Defender for Identity Azure Advanced Threat Protection (ATP)	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, 2008	SNMP: Running Processes	WMI: DHCP metrics: request rate, release rate, decline rate, Duplicate Drop rate etc	FortiSIEM Windows Agent (HTTPS): DHCP logs - release, renew etc;	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
				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 Directort 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 texts; WMI: “repadmin/replsummary” command output - Replication statistics; LDAP: Users with stale passwords, insecure password settings		
Microsoft	Exchange Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage, WMI: Exchange 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		Exchange Tracker Logs via FSM Advanced 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	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
				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 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/Export, Document views, Information Management Policy changes etc	
Microsoft	SQL Server - 2005, 2008, 2008R2, 2012, 2014	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	JDBC: database error log; JDBC: Database audit trail	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
			etc; JDBC: per-instance, per database performance metrics data file size, Log file used, Log growths etc; JDBC: Locking info, Blocking info		
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
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 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	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Mikrotek	Mikrotech Switches and Routes	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, 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,	SNMP: Uptime, Network Interface metrics, Storage Disk Utilization SNMP: Storage Performance metrics: Read rate (IOPS),		

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Hardware model, Serial number, Network interfaces, Physical Disks, Components	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 model, Serial number, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status		
Nutanix	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		
Okta.com	SSO	Okta API: Users		Okta API: Over 90 event types covering user activity in Okta website	
Okta.com	Safeguard		Not supported		
OpenLDAP	OpenLDAP	LDAP: Users			
Oracle	Cloud Access Security Broker (CASB)				

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Oracle	Enterprise Database Server - 10g, 11g, 12c	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 ration, Wait time ration, 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: Listen log, Alert log, Audit Log	
Oracle	MySQL Server	SNMP or WMI: Process resource usage	JDBC: User Connections, Table Updates, tab;e Selects, Table Inserts, Table Deletes, Temp Tab;e 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 Application Server	SNMP or WMI: Process resource usage	JMX: availability metrics, Memory 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	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port	Syslog: Situations covering Authentication Success/Failure,	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Processes, Open Ports; SSH: Hardware details	up/down; SSH: Disk I/O, Paging	Privileged logons, User/Group Modification	
PacketFence	Network Access Control	Host name and Device type	Not supported		Not supported
Palo Alto Networks	Palo Alto Traps Endpoint Security Manager	LOG Discovery	Currently not natively supported	Over 80 event types	Currently no natively supported
Palo Alto Networks	PAN-OS based Firewall	SNMP: Host name, OS, Hardware, Network interfaces; SSH: Configuration	SNMP: Uptime, CPU utilization, Network Interface metrics, Firewall connection count	Syslog: Traffic log, Threat log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs	SSH: Configuration Change
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 Consequences etc	
Qualys	Web Application Firewall			syslog (JSON formatted): web log analysis	
Radware	DefensePro	LOG	Currently not natively supported	Over 120 event types	Currently not

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
		Discovery			natively supported
Rapid7	InsightVM	Host name and Device type	Not supported		
Rapid7	NeXpose Vulnerability Scanner			Rapid7 NeXpose API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bigtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc	
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	
Redhat	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
Redhat	JBOSS	SNMP:	JMX: CPU metrics, Memory	;	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
	Application Server	Process level CPU/Memory usage	metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics		
Redhat	DHCP Server	SNMP: Process level CPU/Memory usage		Syslog: DHCP address release/renew events	
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		
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	Discovered via LOG only	Not natively supported - Custom monitoring needed	System and security events (e.g. file blocked)	Currently not natively supported
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	
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	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Squid	Web Proxy	SNMP: Process level CPU/Memory usage		Syslog: W3C formatted access logs - per HTTP(S) connection: Sent Bytes, Received Bytes, Connection 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
Tigera	Calico	Not natively supported	Not natively supported	Flow, Audit and DNS logs	Not natively supported
TrendMicro	Deep Discovery	Discovered via LOG only	Not natively supported, Custom monitoring needed.	Malicious file detection	Currently not natively supported
TrendMicro	Deep Security Manager			Syslog: Over 10 event types covering end point protection events	Not supported
TrendMicro	Interscan Web Filter	LOG Discovery	Currently not natively supported	15 event Types	Currently not natively supported
TrendMicro	Intrusion Defense Firewall (IDF)			Syslog: Over 10 event types covering end point firewall events	
TrendMicro	Office scan			SNMP Trap: Over 30 event types covering end point protection events - malware/spyware/adware, malicious events	

SUPPORTED DEVICES AND APPLICATIONS BY VENDOR

VENDOR	MODEL	DISCOVERY OVERVIEW	PERFORMANCE MONITORING OVERVIEW	LOG ANALYSIS OVERVIEW	CONFIG CHANGE MONITORING
Vasco	DigiPass			Syslog - Successful and Failed Authentications, Successful and Failed administrative logons	
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	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	
WatchGuard	Firebox Firewall			Syslog: Over 20 firewall event types	
Websense	Web Filter			Syslog: Over 50 web filtering events and web traffic logs	
YXLink	Vulnerability Scanner				