

**Table of Contents**

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2</b>	<b>SERVICE OFFERING.....</b>	<b>3</b>
2.1	SOLUTION PURPOSE.....	3
<b>3</b>	<b>HOW IT WORKS.....</b>	<b>4</b>
3.1	LOGGING.....	5
3.2	COLLECT PARSE AND CORRELATE.....	5
3.3	AUTOMATIC DISCOVERY.....	6
3.4	MULTI-FACETED DATA COLLECTION.....	7
3.5	POWERFUL ANALYTICS FOR REAL-TIME CORRELATION AND ALERTING.....	7
3.6	COMPLIANCE AUTOMATION.....	8
3.7	CMDB AND CHANGE MANAGEMENT.....	9
3.8	CMDB FEATURES.....	9
3.9	CHANGE MANGEMENT FEATURES.....	9
3.10	RUNNING AND STARTUP CONFIGURATION.....	10
3.11	CONFIGURATION DFF.....	10
3.12	INCIDENT NOTIFICATION OVERLAY.....	10
3.13	IDENTITY LOCATION MANAGEMENT.....	11
3.14	KNOW THE USER AND LOCATION – NOT JUST THEIR IP ADDRESS.....	11
3.15	PORT IDENTITY.....	12
3.16	LAYER 2 TOPOLOGY WITH LOCATION.....	12
<b>4</b>	<b>INSTALLATION AND CONFIGURATION.....</b>	<b>12</b>
4.1	INSTALLATION.....	12
4.2	EASY TO SCALE.....	13
4.3	INITIAL CONFIGURATION.....	13

<b>5</b>	<b>SECURITY SERVICES</b> .....	<b>13</b>
5.1	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SERVICE   CORE SERVICE.....	13
5.2	SERVICE LEVEL OBJECTIVE .....	13
5.3	SYSTEM TUNING.....	13
5.4	MONTHLY SECURITY ADVISORY .....	14
5.5	INCIDENT INVESTIGATION.....	14
5.6	COVERAGE LIMITATIONS.....	14
5.7	COMPLIANCE REVIEW SERVICE .....	14
<b>6</b>	<b>MATRIX OF SERVICE PACKAGES</b> .....	<b>15</b>
<b>7</b>	<b>SERVICE UNIFORMITY</b> .....	<b>15</b>
<b>8</b>	<b>TECHNICAL SUPPORT AND MONITORING</b> .....	<b>15</b>
<b>9</b>	<b>SERVICE LIMITATIONS</b> .....	<b>15</b>
<b>10</b>	<b>VIRTUAL APPLIANCE</b> .....	<b>16</b>
<b>11</b>	<b>REPORTING</b> .....	<b>16</b>
<b>12</b>	<b>APPENDIX A</b> .....	<b>17</b>
<b>13</b>	<b>APPENDIX B</b> .....	<b>17</b>

## 1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Security Information and Event Management, or SIEM-as-a-Service (the "Service").

The service definitions found herein reflect Synoptek's standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect the current Synoptek best practices or industry standards at its sole discretion with or without notice.

## 2 SERVICE OFFERING

Synoptek's Security Services are designed to defend and minimize your attack surface. Our Security Services include threat detection, investigation, and reporting. Our Security personnel will continue to advise on ever changing threats and recommended actions.

Synoptek's Security Information and Event Management services, or SIEM-as-a-Service, is designed to provide organizations all the benefits needed from a security information and event management system without any of the headache or capital investment. The offering is a comprehensive SIEM-as-a-Service solution, fully hosted in a secure and compliant cloud to manage and monitor your critical systems regardless of where they may be.

Key Features:

- Fully hosted & managed SIEM
- Comprehensive device support
- Event log consolidation
- In-depth security and anomalous activity monitoring
- Pre-tuned rules
- Ongoing rule enrichment
- Ongoing rule tuning and false-positive reduction
- Managed upgrades to SIEM
- No capital expenditures
- Device onboarding
- Virtual CISO service

### 2.1 SOLUTION PURPOSE

Most organizations don't have the technology or personnel to detect these cybersecurity threats, let alone investigate or remediate them. The average time between a data breach and discovery is 205 days. Simply implementing security tools such as firewalls or anti-virus isn't enough. This is even more true for organizations that fall under PCI, HIPAA, SOX, or FFIEC regulations. For those companies, compliance with various guidelines and mandates is absolutely critical to avoid fines or worse.

Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation. That technology is known as security

information and event management (SIEM), and it provides deep security intelligence for your IT environment. A proper SIEM solution can help answer critical questions that are vital to your cybersecurity protection – questions such as:

- A user login has failed multiple times; did the employee forget their password or is this a brute force attack?
- Sensitive files on a server were accessed last night; is this normal business use or did we just get breached?
- A typical firewall can send out 864,000 events per day; how do I know which of these (if any) are important?
- New wireless access points have been added to the network; where are they and was this intentional?
- Are our employees going to sites – intentionally or not – that put us at risk for malware infection?
- Regulatory compliance requirements are changing constantly; do we have the data needed to properly comply?

### 3 HOW IT WORKS

Synoptek provides automated alert handling and notifications with human oversight for on-premise devices including firewalls, routers, unified threat management devices, switches, servers and all other devices for which there is a preconfigured SIEM parser. Security alerts generated by Client's device(s) will be sent directly to the SIEM for collection and correlation via an on-premise Collector (minimum of one required per end customer organization; requires virtualization). Notifications will then be automatically sent to configured contacts via email, based on Client's Incident Notification Policy.

With an integrated and cross-correlated view into your network, devices, apps and user logs, Synoptek simplifies the collection of information that impacts your business. With a powerful analytics engine, automated CMDB and event consolidation, smart anomaly detection, identity and location binding, and flexible data management, we redefine the next generation of SIEM.

Synoptek delivers a robust, scalable SIEM-as-a-Service solution:

- Mainstream device support
- Event source monitoring
- Event log and network flow data consolidation
- Comprehensive, extensible analytics
- Network, virtualization, and application intelligence
- Identity and location intelligence
- Configuration and configuration change monitoring
- In-depth database security, availability and anomalous activity monitoring
- Powerful, layer 7 rules engine
- Real-time and historical cross-correlation
- Prioritized, valid security incidents with correlated and raw details
- Dynamic dashboards, topology maps and notification
- Real-time and long-term search with web-like query and iterative filtering
- Directory service integrated and custom asset and user grouping
- Compliance and standards-based reports
- Optimized event repository
- Event log data integrity secured by HMAC

The Security Information and Event Management (SIEM) platform is hosted by Synoptek and offers:

- Redundant, geographically disperse datacenters
- Nightly data replication between datacenters
- Three (3) month data retention within the portal; additional storage length is available for an additional fee

### 3.1 LOGGING

Event log management / security information event management (SIEM) is considered an IT best practice, and for regulated industries, an audit compliance requisite.

The challenge is how to consistently aggregate, decipher and normalize non-standard log formats; manage massive volumes of event log data for real-time and historic analysis; correlate and consolidate complex event log data to yield actionable intelligence; and maximize event log value to support IT service reliability.

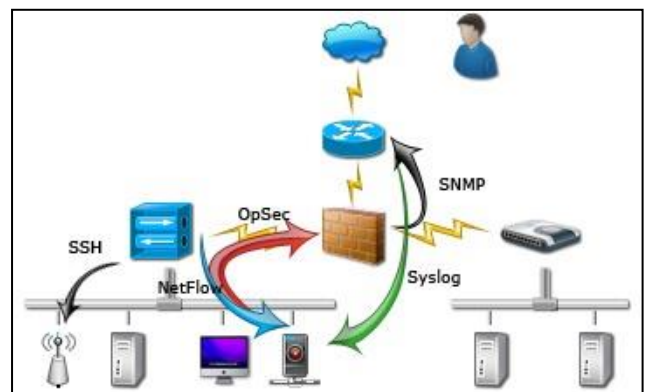
Some equate log management to log aggregation, display, and storage – a simple approach that fails to address these complex challenges. Most SIEM products offer basic event consolidation, simple correlation rules, limited real-time analysis, poor reporting and investigation flexibility, and no identity or infrastructure context. Many still require special collectors, add-on modules, additional systems and significant expertise. None of this is required for Synoptek’s SIEM-as-a-Service.



### 3.2 COLLECT PARSE AND CORRELATE

Supporting multi-vendor device sources and advanced parsing technology, Synoptek can collect, parse, correlate and store logs from virtually all your IT infrastructure sources. Our solution automatically interprets the device type and how to process the event logs as they are received.

- *Network activity logs* from Firewalls, Routers, Switches, VPN Gateways, Wireless LAN, Web/Mail Security Gateways, and Network IPS
- *Network resource utilization* and anomaly detection from network flow data
- *Server operating system* security logs from Windows, Unix, Linux and virtual machines




- Network infrastructure *application logs* from domain controllers, authentication servers, DNS and DHCP servers, and vulnerability management servers
- *User application logs* from web, application, and database servers

Synoptek's parsers intelligently categorizes the source of the log into different device groups such as Firewalls, Routers / Switchers, Wireless LAN Controllers, Printers, etc. It also groups into various server categories such as Windows, Unix, VMWare, and storage devices.

**A list of covered sources will be included in your Synoptek Service Order.**

### 3.3 AUTOMATIC DISCOVERY

With our solution, Synoptek automatically discovers your network infrastructure and its resources using intelligent scanning methods. It supports a smart scan method, which iteratively learns only about the live devices in your network. Since only live devices are traversed, it is much faster than other traditional methods of network security and device discovery. It also supports a range scan method where each machine in the range is first pinged and then an attempt is made to do full discovery using the given credentials. Once the capabilities of the devices are known, the security information which can be fetched from those devices are automatically determined.

Step 1: Enter Credentials 		
Name	Protocol	Device Type
Community-String-Win	SNMP	Generic
dc-wmi	WMI	Microsoft Windows
Foundry-Telnet	TELNET	Foundry Ironware
Foundry-Telnet-enable	TELNET	Foundry Ironware
IOS-Ssh-Username-PW	SSH	Cisco IOS
IOS-Ssh-Username-PW-ePW	SSH	Cisco IOS
IOS-Telnet-PW-ePW	TELNET	Cisco IOS
IOS-Telnet-Username-PW	TELNET	Cisco IOS
jmx	JMX	SUN Glassfish App Server
LDAP	LDAP	Generic
oracle db	JDBC	Oracle Database Server
PIX/ASA-Username-PW-ePW	SSH	Cisco IOS
SNMP Generic	SNMP	Generic

### 3.4 MULTI-FACETED DATA COLLECTION

Synoptek supports virtually all agent-less and agent-based data collection methods to collect logs from a variety of devices and applications including:

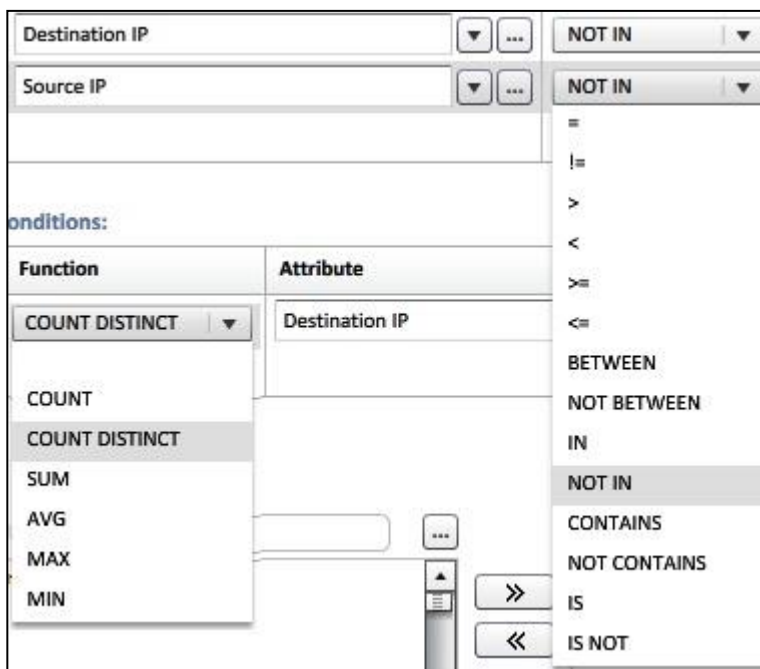
- SNMP
- Syslog
- Windows Management Instrumentation (WMI)
- Microsoft RPC
- Cisco SDEE
- Checkpoint LEA
- JDBC
- VMWare VI-SDK
- JMX
- Telnet
- SSH
- HTTPS
- IMAP / IMAP over SSL

### 3.5 POWERFUL ANALYTICS FOR REAL-TIME CORRELATION AND ALERTING

Synoptek can detect your network services and profile network traffic from network flows and firewall logs. An advanced analytics engine detects patterns in data over a rolling time window taking into account very complex patterns. This includes combined patterns of network, system, application and user activity. The built-in analytics engine can be easily extended using XML-based definitions.

Synoptek’s solution contains more than 500 built-in rule classes which cover scenarios such as:

- Host scans, port scans, fixed-port host scans, denied scans, and other traffic anomalies
- Network device and server logon anomalies
- Network access anomalies from VPN, domain controller and wireless logons
- Web server and database access anomalies
- Rogue workstations, mobile devices, and WLAN APs etc. from DHCP logs
- Account lockouts, password scans, and unusual failed logon patterns
- Botnets, mail viruses, worms, DDOS, and other day zero malware from DNS, DHCP, web proxy logs, and flow traffic



The analytics engine patterns are comprehensive and allow us to build complete Boolean operators and nested sub-pattern rules:

- Sub-patterns connected in the time dimension by operators such as AND, OR, FOLLOWED\_BY, AND\_NOT, NOT\_FOLLOWED\_BY
- Each sub-pattern can apply condition operators such as =, !=, BETWEEN, IN, NOT IN, IS, IS NOT, etc
- Each sub-pattern can filter and apply aggregation operators such as AVG, MAX, MIN, COUNT, and COUNT DISTINCT
- The thresholds can be static or statistically derived from automatically profiled data

### 3.6 COMPLIANCE AUTOMATION

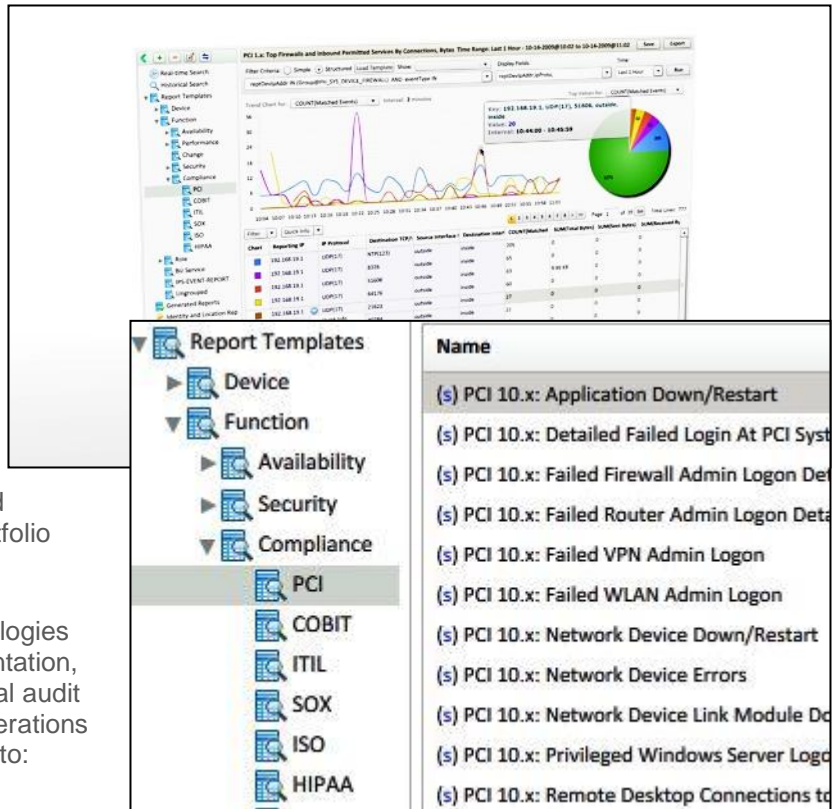
Synoptek offers full log aggregation, real-time event correlation, and online data retention with rules and reports mapped to compliance standards such as PCI, FFIEC, SOX, and HIPAA.

By incorporating an automated CMDB, statistical profiling, and true identity binding for complete access records, Synoptek automates your audit and control processes.

Standards and compliance are all about implementing policies, procedures, and technologies that reduce business risk, as well as being able to efficiently validate that controls are working according to stated policy expectations and mandated requisites. Beyond setting policy and procedures, many tools in an IT's management portfolio must support compliance efforts.

The question then becomes finding the right technologies that best automate control verification and documentation, as well as those that streamline internal and external audit challenge/response processes. Compliance considerations for IT management tools should include the means to:

- Validate a broad set of policies across technologies
- Deliver on-demand results to auditor inquiries
- Readily obtain applicable data and documentation
- Normalize compliance-relevant data across disparate systems
- Diminish compliance liabilities and audit duration
- Meet auditing and data management standards
- Identify control gaps and prioritize incident response
- Adapt to existing security, governance and auditing processes
- Respond to complex and rapidly changing environments





Synoptek satisfies all the above compliance considerations with built-in dashboards, analytics, and reports mapped to leading standards and compliance best practices.

### 3.7 CMDB AND CHANGE MANAGEMENT

Synoptek’s solution delivers a fully automated and comprehensive CMDB – discovering, intelligently grouping and maintaining a smart inventory of network assets, software, patches, users and directory objects. And we build all this directly from your infrastructure and trusted sources without requiring agents.

### 3.8 CMDB FEATURES

Synoptek’s solution discovers, records, monitors, and reports on all your network assets, both physical and virtual. Our solution allows organizations to quickly and easily:

- Track hardware and software assets
- Understand what software is installed and what is running
- Analyze system utilization by application and respective processes
- Associate asset allocation with users, groups and services
- Monitor network application use and resource consumption by user or group
- Track blacklist or whitelist applications
- Assess and integrate patch deployment and vulnerability issues
- Identify shelfware and license reduction opportunities
- Plan capacity and migration options for consolidation projects
- Prepare for audits

Statistics			
Created at	Tue Sep 22 2009 5:57:34 PM via LOG		
Last Updated at	Fri Oct 9 2009 6:31:39 PM via MANUAL		
# Interfaces	<u>2</u>	# Components	<u>0</u>
# Installed S/Ws	<u>20</u>	# Running Apps	<u>113</u>
# System Services	<u>114</u>	# Patches	<u>104</u>
# Processors	<u>2</u>	# Storage	<u>4</u>

General	
Name	Ads-Pri-Win-Server
Access IP	192.168.0.10
Type	Microsoft Windows Server 2003
Version	Service Pack 2
OS Serial#	69712-347-7780742-42014
Build #	5.2.3790
Importance	Critical
Owner/Org	IT Dept
Location	SJC/Building#2, Floor#1, Lab#5, Rack#14

### 3.9 CHANGE MANGEMENT FEATURES

As a part of Change Management, Synoptek detects the following scenarios:

- Monitors network device configurations for startup configuration change and difference between startup and running configuration
- Monitors installed software differences for new software installations and existing software uninstalls
- Monitors active directory user/group membership changes
- Stores *versioned* configuration in database
- Alerts on configuration changes, tied together with admin IP and workstation
- Alerts on unauthorized changes
- Reports on configuration change history, optionally by business service

### 3.10 RUNNING AND STARTUP CONFIGURATION

As a part of change management, Synoptek discovery module discovers the "start-up" and "running configuration" from the network devices such as routers, firewalls and switches over a historical period. It intelligently detects the difference between the startup configuration and running configuration and differences between various startup configurations over a long period of time.

Interface VLAN1 ip address 172.16.10.254 2! no ip directed-broadcast no ip route-cache ! ip default-gateway 172.16.1 logging 172.16.21.75 snmp-server engineID local snmp-server community pu snmp-server location PH-Q/ snmp-server contact WenYi	Interface VLAN1 ip address 172.16.10.254 2! no ip directed-broadcast no ip route-cache ! ip default-gateway 172.16.1 logging 172.16.21.75 logging 100.1.1.1 snmp-server engineID local snmp-server community pu snmp-server location PH-Q/
--	--

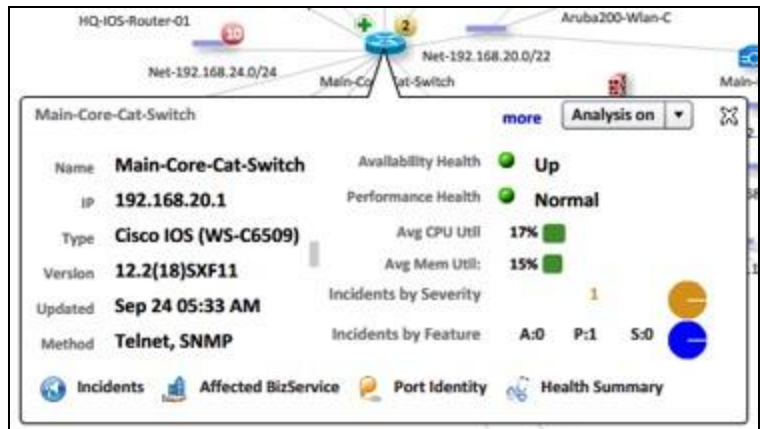
Whenever a change is detected, it creates an incident and notifies the administrator about the change. With this intelligence, the administrator can keep track of the changes done which are unauthorized configuration changes to their core network devices. The administrator can look at the configuration of any historical time interval, by selecting the revision of that configuration.

### 3.11 CONFIGURATION DIFF

It is also possible to view the versioned configuration at any time, and is possible to search for specific keywords in the configuration. Using an intuitive UI, the administrator can also **diff** between any version of the running configuration. With this feature, it's very easy to detect changes and to pinpoint each specific change in the configuration.

### 3.12 INCIDENT NOTIFICATION OVERLAY

The Synoptek system keeps track of the incidents occurring on your network using an advanced analytics engine in real-time. Synoptek can write a rule to detect any simple or complex scenario and the system will create the correct alerts applicable to that scenario. The visualization engine automatically keeps track of these incidents and overlays them on the main graph nodes so that the user can get a rapid visual cue of network issues at any time. The tool has the option of showing all incidents – critical (red) incidents, warning (yellow), or informational (green) incidents. These topology **incident overlays** are automatically updated by the user interface. It's also possible to obtain full details on each incident, by just clicking on the *incident count indicator button*.



### 3.13 IDENTITY LOCATION MANAGEMENT

Using an innovative identity and location-to-event binding technology, Synoptek automatically associates IP addresses to machine names, MAC addresses, switch VLAN IDs, logged-on users and directory objects. Now complete who and where details are maintained as action records, irrespective of the use of shared credentials, including the network the user has connected to and by what method.

Analytics > Identity and Location Report		
(636 of 636)		
IP address	User	Location
192.168.0.26	sdickinson (Domain)	Main-Core-Cat-Switch 192.168.20.1 (GigabitEthernet6/12)
192.168.20.52	elee (Domain)	
192.168.20.39	ayong (Domain)	
192.168.0.26	apacheSVN (Domain)	Main-Core-Cat-Switch 192.168.20.1 (GigabitEthernet6/12)
192.168.0.26	phoenix_dev (Domain)	
192.168.0.10	Administrator (Domain)	Main-Core-Cat-Switch 192.168.20.1

### 3.14 KNOW THE USER AND LOCATION – NOT JUST THEIR IP ADDRESS

Using identity and location-to-event binding technology, Synoptek intelligently associates IP addresses to machine names, MAC addresses, switch VLAN IDs, logged on user name, and directory identity. It automatically identifies a user's location in terms of nearest WLAN AP, controller, VPN gateway, Layer 2 switch port, and associates primary logins to secondary logins in order to identify the real user behind administrative accounts. With this information, any IP address can be automatically associated to a specific user, on a specific server/laptop, and connected to the network via a specific access method: AAA, VPN or switch.

By binding user identity and location to events, full who and where details are maintained as an action record irrespective of the use of shared credentials. Now investigating operational issues, change anomalies, security breaches and violations, and reporting on internal user actions are no longer obstacles.

These actionable identity and location details are presented, used and always available in dashboards, topology maps, incidents, enterprise search, rules and reports. As changes in directory objects, new network devices and systems, or known or unknown users access your infrastructure, all the pertinent location and identity information is current and maintained for real-time and historic analysis.

**SJ-QA-Service-IOS** more Analysis on

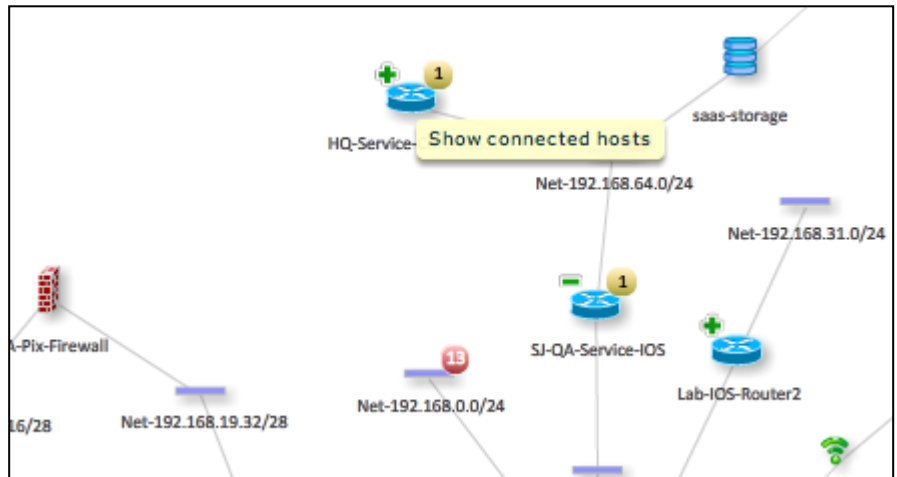
Name: <b>SJ-QA-Service-IOS</b>	Availability Health: <span style="color: green;">●</span> <b>Up</b>
IP: <b>192.168.19.50</b>	Performance Health: <span style="color: green;">●</span> <b>Normal</b>
Type: <b>Cisco IOS (CISCO2801)</b>	Avg CPU Util: <b>24%</b>
Version: <b>12.4(1c)</b>	Avg Mem Util: <b>16%</b>
Updated: <b>Sep 23 10:51 PM</b>	Incidents by Severity: <b>1</b>
Method: <b>Telnet, SNMP</b>	Incidents by Feature: <b>A:0 P:1 S:0</b>

[Incidents](#)
[Affected BizService](#)
[Port Identity](#)
[Health Summary](#)

### 3.15 PORT IDENTITY

Synoptek keeps track of the MAC to VLAN ID mapping in switches and routers, so that it can map an IP address to a specific machine name, MAC/VLAN ID, and logged on user.

In this way, Synoptek provides the server (or host) connected to each port along with the corresponding IP address, user (VPN, Domain or AAA), location (switch or wireless controller), and the last and first seen time information.



### 3.16 LAYER 2 TOPOLOGY WITH LOCATION

Synoptek can visualize your layer 2 topology for each switch or router along with VLAN ID and server information directly in the Synoptek Topology View. By clicking on the '+' icon on any switch or router in the Topology view, the latest layer 2 topology information for that device will be shown immediately to the Synoptek analyst.

The dynamic user identity and location mapping also helps to improve incident response time, investigations, planning, and operational changes. The identity and location information along with the historic event details can be exported into PDF or CSV formats and emailed to the applicable administrator.

## 4 INSTALLATION AND CONFIGURATION

### 4.1 INSTALLATION

Synoptek installation can be scheduled to be performed within a 4-hour service window and is non-disruptive to your systems. The SIEMaaS collector is a virtual appliance that is capable of operating on ESX, KVM or HyperV. The collector will require at least 2 cores, 4GB of memory and 40gb of hard drive space. A virtual machine will need to be provisioned for Synoptek's use. In the event that a virtual machine is not available an appliance can be provided.

## 4.2 EASY TO SCALE

A single appliance can take multiple inputs of network traffic and cover up to tens of thousands of individual machines, depending on peak traffic volumes.

## 4.3 INITIAL CONFIGURATION

The SIEM initially takes 4-6 weeks to become effective effectively tuned. Ongoing tuning, which is included in the service, will progressively provide improvement in data quality.

# 5 SECURITY SERVICES

## 5.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SERVICE | CORE SERVICE

Synoptek's Security Information and Event Management (SIEM) service includes 24x7x365 automated monitoring and alerting through advanced log correlation, contextual analytics, big data analysis and Synoptek's custom-tuned rule database. Synoptek's robust, scalable solution provides you with automated notifications with human oversight for on-premise devices including firewalls, routers, unified threat management devices, switches, servers and all other devices for which there is a preconfigured SIEM parser (See Appendix B for list of available parsers).

## 5.2 SERVICE LEVEL OBJECTIVE

Synoptek will continuously monitor for threats as presented by the SIEM. Threat indicators will be assessed, and incidents will be categorized into three levels of severity. The most detrimental threats are categorized with the moniker "Severe Threat" (ST), and for those, Synoptek will gather and document the necessary context and activity logs required to act. Notification will be provided in writing to the customer's designated alert contact. See Appendix A for Threat Indicator Levels and their associated definitions.

## 5.3 SYSTEM TUNING

Synoptek is responsible for detecting network anomalies and sorting out the bad traffic patterns from among the vast false positive bad traffic patterns that show up on our screens hourly. As a result, Synoptek has its interests aligned with those of its clients to reduce false positives and increase the signal to noise ratio of potential threats. An initial 4-6 weeks of tuning are required before the system becomes effective. Ongoing tuning, which is included in the service, will progressively provide improvement in report data quality.

#### 5.4 MONTHLY SECURITY ADVISORY

This service includes a Monthly recurring information security review meeting. In this meeting, Synoptek will lead a review of the prior Month's threats, discuss any new threat vectors, and recommended changes to systems or policies. This will be conducted via a conference call.

#### 5.5 INCIDENT INVESTIGATION

Synoptek's Incident Analysts are experts in defence, intelligence and interpreting suspicious activities around probable threats. This process includes analysing traffic entering, leaving as well as traversing within your network. Incident analysis of this kind is often like finding a needle in a hay stack and requires skills and understanding far beyond the normal abilities of most network professionals.

For every incident received, our analysts draw on their expertise, external sources of intelligence and the context of the network before taking an informed action on the threats faced. Investigation activities include detailed log analysis, and looking for suspicious trends.

Synoptek will open a ticket for each incident with a threat indicator of High Threat or Severe Threat. Threat indicators of Severe Threat will be opened as a service ticket with an initial priority of 'P2 – User Expedite'. Threat indicators of High Threat will be opened as a service ticket with an initial priority of P3. Service ticket investigation work will be performed in accordance with the Synoptek Managed Services SLA. Service Ticket priority levels may change during the course of Synoptek's investigation.

#### 5.6 COVERAGE LIMITATIONS

This service includes investigation for all incidents with threat indicators of either High Threat (Ticket opened as P3) or Severe Threat (Ticket opened as 'P2 – User Expedite'). Due to the variable nature of security incident investigation, tickets opened for investigation shall be worked until root cause analysis can be identified, up to 5 hours.

#### 5.7 COMPLIANCE REVIEW SERVICE

With this additional service, Synoptek's Compliance Review Service provides monitoring and response that meets regulatory requirements for PCI, FFIEC and HIPAA. With this service, you receive a dedicated team of Synoptek's security analysts who perform daily review of all your logs and notifications, 7 days a week, 365 days a year. Each day's review is tracked and logged to prove regulatory compliance. If any significant issues are found during the daily review, a notification is created and sent to you.

## 6 MATRIX OF SERVICE PACKAGES

Service Name	Package Details
SIEM-as-a-Service	SIEM Service
SIEM + Compliance	SIEM + Compliance Review Service

## 7 SERVICE UNIFORMITY

Synoptek's SIEM as a Service allows you the flexibility to choose the service package that's right for you and your organization. As such, once you've made a service selection, that selection holds true for a minimum 12 months from the service start date. For example, you select the SIEM Service, but you can still choose to add Compliance Review later; doing so, however, refreshes the 12-month minimum timeframe before your service package could scale back.

In addition to the above, all subscribed devices must maintain the same unified service package across the subscription. For example, in order for any device to subscribe to either the Compliance Review Service or SIEM Service, all subscribed devices would need to adhere to the same service package. Preference is given to the Compliance Review Service in the event that a change order or other service altering request is made that does not fully comply with the above.

## 8 TECHNICAL SUPPORT AND MONITORING

Synoptek will provide support for troubleshooting and resolution for the local appliance that will be monitored by Synoptek's Security Services Team. In addition, a web-based ticketing system to support tickets, track, and provide correspondence for any support related issue. All communication will be handled through the Ticket System.

Synoptek will remediate issues related to the local appliance, identified either via monitoring and notification, or those initiated through contacting the Service Desk. In both cases, a service ticket will be created and prioritized based on severity. The service desk will attempt to resolve the issue remotely, escalating to level 2, then level 3 engineers as required. If the issue cannot be resolved remotely, a field technician will be dispatched.

## 9 SERVICE LIMITATIONS

Synoptek's SIEM as a Service is an excellent addition to an organization's strategy of defense in depth. Some threat attack users and systems in ways that may not immediately present any detectable network traffic. As a result, this service alone cannot detect all threats and is best used in conjunction with other protective measures. Not all threats create anomalous network activity and thus will not be detected and reported. Furthermore, this service differs from a threat prevention service in that it is meant to detect the threats that manage to bypass your other security systems and protective barriers. While this service cannot prevent any intrusion, its utility is in early detection, and investigation.

Note that while access to the SIEM is limited to Synoptek staff, it may be presented to customer staff in monthly threat advisories as well as when presenting critical threat information.

## 10 VIRTUAL APPLIANCE



It is important to reiterate that the SIEM Collector is a Virtual Appliance. If the target environment does not currently support virtualization and hardware needs to be procured to facilitate installation of the Collector, the expense of said hardware will be outside of the price of the SIEMaaS offering.

## 11 REPORTING

You will receive a Monthly Threat Intelligence Report.



12 APPENDIX A

<u>Severity Icon</u>	<u>Description</u>
	<p><b><u>Severe Threat</u></b> Any incident (ongoing or detected) that has been determined to have the potential for severe commercial, legal and/or operational impact.</p> <p>Severe Threats are those that should be raised to the executive level immediately as data and/or resource confidentiality, integrity and/or availability are at significant risk.</p>
	<p><b><u>High Threat</u></b> Any incident (ongoing or detected) that has been determined to have the potential for moderate commercial, legal and/or operational impact.</p> <p>High Threats are those that could indicate malicious use of corporate resources, are active infections or are otherwise placing the organization's data and/or resource confidentiality, integrity and/or availability at moderate risk.</p>

13 APPENDIX B

<u>Vendor</u>	<u>Model</u>
<b>3Com</b>	TippingPoint UnityOne IPS
<b>3Com</b>	TippingPoint Security Management System
<b>Adtran</b>	NetVanta
<b>Adtran</b>	Multiplexer
<b>AirTight</b>	SpectraGuard
<b>AirWatch</b>	MDM
<b>AKCP</b>	SensorProbe

<u>Vendor</u>	<u>Model</u>
<b>Avaya</b>	Session Manager
<b>Avaya</b>	Media Gateway
<b>Barracuda</b>	Spam Firewall
<b>Bit9</b>	Security Platform
<b>Bit9</b>	Carbon Black
<b>Blue Coat</b>	SGOS Web Proxy
<b>Blue Coat</b>	CacheOS

<b>Alcatel-Lucent</b>	TiMOS
<b>Alcatel-Lucent</b>	AOS
<b>Alcatel-Lucent</b>	8950 AAA
<b>Amazon</b>	AWS EC2
<b>Amazon</b>	AWS CloudTrail
<b>Amazon</b>	AWS RDS
<b>Apache</b>	Apache Tomcat
<b>APC</b>	UPS
<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>APC</b>	PDU
<b>APC</b>	Generic
<b>APC</b>	NetBotz
<b>APC</b>	NetBotz Rack Monitor
<b>Apple</b>	Mcintosh
<b>Apple</b>	Mac OSX
<b>Apple</b>	iOS
<b>Arista</b>	EOS

<b>Box.com</b>	Box
<b>Brocade</b>	San Switch
<b>Brocade</b>	ServerIron ADX
<b>BSDI</b>	BSD OS
<b>Caldera</b>	OpenLinux
<b>CentOS</b>	Linux
<b>Checkpoint</b>	FireWall-1
<b>Checkpoint</b>	SmartCenter
<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>Checkpoint</b>	Virtual Firewall
<b>Checkpoint</b>	VSX
<b>Checkpoint</b>	Provider-1 MDS
<b>Checkpoint</b>	Provider-1 CMA
<b>Checkpoint</b>	Provider-1 CLM
<b>Checkpoint</b>	Provider-1 MLM
<b>Checkpoint</b>	UTM-1 Edge
<b>Checkpoint</b>	IPSO

<b>Aruba</b>	ArubaOS WLAN AP
<b>Aruba</b>	ArubaOS WLAN Controller
<b>Aruba</b>	ClearPass PolicyManager
<b>Astaro</b>	Security Gateway
<b>Avaya</b>	ERS
<b>Avaya</b>	Communication Manager

<b>Checkpoint</b>	Firewall-1 SPLAT
<b>Checkpoint</b>	FireWall-1 GAIA
<b>Cisco</b>	ASA
<b>Cisco</b>	PIX
<b>Cisco</b>	FWSM
<b>Cisco</b>	IPS

<u><b>Vendor</b></u>	<u><b>Model</b></u>
<b>Cisco</b>	CSA Management Center
<b>Cisco</b>	IOS
<b>Cisco</b>	CatOS
<b>Cisco</b>	NX-OS
<b>Cisco</b>	ACE
<b>Cisco</b>	WLAN AP
<b>Cisco</b>	WLAN Controller
<b>Cisco</b>	IOS WLAN AP
<b>Cisco</b>	IOS WLAN Controller

<u><b>Vendor</b></u>	<u><b>Model</b></u>
<b>Cisco</b>	Meraki Firewall
<b>Cisco</b>	Meraki Switch
<b>Cisco</b>	WAAS
<b>Cisco</b>	FireAMP
<b>Cisco</b>	FirePOWER
<b>Cisco</b>	Telepresence Video Comm Server
<b>Cisco</b>	CiscoWorks NCM
<b>Cisco</b>	FireAMP Cloud
<b>Citrix</b>	Presentation Server

<b>Cisco</b>	IronPort AsyncOS Mail
<b>Cisco</b>	Cisco Secure ACS
<b>Cisco</b>	VPN 3K
<b>Cisco</b>	SAN-OS
<b>Cisco</b>	Call Manager
<b>Cisco</b>	Unity Connection
<b>Cisco</b>	UCS
<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>Cisco</b>	CleanAccess
<b>Cisco</b>	ONS
<b>Cisco</b>	BOS
<b>Cisco</b>	VoIP Phone
<b>Cisco</b>	IronPort AsyncOS Web
<b>Cisco</b>	CBOS
<b>Cisco</b>	Presence Server
<b>Cisco</b>	Contact Center
<b>Cisco</b>	Tandberg VCS

<b>Citrix</b>	NetScaler
<b>Compuware</b>	Dynatrace App Monitoring
<b>Conectiva</b>	Linux
<b>Cradlepoint</b>	Router
<b>Cray</b>	Unicos
<b>Crypto AG</b>	Link Encryption
<b>CyberArk</b>	Enterprise Password Vault
<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>Cylance</b>	Protect
<b>Cyphort</b>	Cortex
<b>Damballa</b>	Failsafe
<b>Debian</b>	Linux
<b>Dell</b>	MFP
<b>Dell</b>	EqualLogic
<b>Dell</b>	Blade Server
<b>Dell</b>	Force10
<b>Dell</b>	Compellent Storage

<b>Cisco</b>	Telepresence MCU
<b>Cisco</b>	LWAPP WLAN Controller
<b>Cisco</b>	Meraki Cloud Controller
<b>Cisco</b>	Meraki WLAN AP

<b>Dell</b>	PowerConnect
<b>Dell</b>	NSeries
<b>Eaton</b>	PDU
<b>EMC</b>	RSA Authentication Manager

<b><u>Vendor</u></b>	<b><u>Model</u></b>
EMC	Clariion
EMC	VNX
EMC	Data Domain
EMC	Generic
Enterasys	Switch/Router
ESET	Nod32
Extreme	Extremeware
Extreme	XOS
F5	Big-IPOS
Fedora	Linux
FireEye	MPS
FireEye	HX
ForeScout	CounterACT
Fortinet	FortiSIEM
Fortinet	FortiOS
Fortinet	FortiManager

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Google	Android
Google	ChromeOS
Green League	WVSS
Green League	RSAS
H3C	Comware
HP	ProCurve
HP	HPUX
HP	JetDirect
HP	LaserJet
HP	Tru64 Unix
HP	OpenVMS
HP	True64 Unix
HP	BladeSystem
HP	VSeries
HP	3Com Switch
Huawei	VRP

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>Foundry</b>	Ironware
<b>FreeBSD</b>	FreeBSD
<b>Freshmeat-org</b>	syslog-ng
<b>Generic</b>	Generic
<b>Generic</b>	JEE App Server
<b>Generic</b>	Linux DHCP
<b>Generic</b>	DHCP
<b>Generic</b>	Linux
<b>Generic</b>	Unix
<b>Generic</b>	Printer
<b>Generic</b>	Android
<b>Generic</b>	Postfix
<b>Gentoo</b>	Linux

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>IBM</b>	ISS Proventia
<b>IBM</b>	ISS RealSecure
<b>IBM</b>	ISS SiteProtector Mgmt Server
<b>IBM</b>	AIX
<b>IBM</b>	DB2
<b>IBM</b>	WebSphere App Server
<b>IBM</b>	OS400
<b>IBM</b>	Guardium
<b>Imperva</b>	Securesphere DB Monitoring Gateway
<b>Imperva</b>	Securesphere DB Security Gateway
<b>Imperva</b>	Securesphere Web App Firewall
<b>Imperva</b>	Securesphere MX Management Server
<b>InfoBlox</b>	NiOS

<b><u>Vendor</u></b>	<b><u>Model</u></b>
ISC	BIND DNS
Isilon	OneFS
Juniper	SSG ScreenOS
Juniper	Netscreen ScreenOS
Juniper	Security Central Manager
Juniper	Netscreen IDP
Juniper	JunOS
Juniper	Steel-Belted RADIUS
Juniper	Secure Access
Juniper	SRX JunOS
Juniper	DDoS Secure
Lantronix	SLC Console Manager
Liebert	HVAC
Liebert	UPS
Liebert	FPC
Mandrakesoft	Mandrake Linux

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Microsoft	Windows XP
Microsoft	Windows Vista
Microsoft	Windows Server 2008
Microsoft	Windows Server 2000
Microsoft	SQL Server
Microsoft	IIS
Microsoft	Exchange Server
Microsoft	IAS
Microsoft	DNS
Microsoft	DHCP
Microsoft	TCP/IP Services
Microsoft	Windows NT
Microsoft	Domain Controller
Microsoft	PPTP/L2TP VPN
Microsoft	Virtual PC 2005
Microsoft	Windows 7



<b><u>Vendor</u></b>	<b><u>Model</u></b>
McAfee	Intrushield
McAfee	ePolicy Orchestrator
McAfee	Common Management Agent
McAfee	Host Intrusion Protection for Servers
McAfee	Host Intrusion Protection for Desktops
McAfee	Sidewinder Firewall
McAfee	WebGateway
McAfee	Vulnerability Manager
McAfee	Reconnex iGuard
McAfee	Stonesoft IPS
Microsoft	ISA Server
Microsoft	Windows
Microsoft	Windows Server 2003

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Microsoft	Windows 98
Microsoft	Windows Me
Microsoft	Virtual Server 2005
Microsoft	Virtual PC 2004
Microsoft	Virtual PC 2007
Microsoft	SharePoint
Microsoft	Windows 8
Microsoft	Windows Server 2012
Microsoft	Forefront UAG
Microsoft	Windows Server 2008 R2
Microsoft	Windows Server 2012 R2
Microsoft	Windows Server 2003 R2
Microsoft	Azure Audit

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Microsoft	Azure Compute
MikroTik	RouterOS
Motorola	WiNG WLAN AP
Motorola	AirDefense
Nagios	Mgmt Server
nCircle	Suite360 Scanner
NetApp	DataONTAP
NetBSD	NetBSD
NetMotion	Mobility XE
Nginx	Web Server
Nimble Storage	NimbleOS
Nortel	BayStack
Nortel	AlteonOS
Nortel	ERS
Nortel	Passport
Novell	Netware

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Panasonic Aero	Content Server
Panasonic Aero	Cabin Terminal
Panasonic Aero	Area Distribution Box
Panasonic Aero	Aircraft Interface
Panasonic Aero	Generic
pfSense	BSD Firewall
Postgres	PostgreSQL
Pulse Secure	Pulse Connect
QNAP	Turbo NAS
Qosmos	DeepFlow
Qualys	QualysGuard Scanner
Qualys	Web Application Firewall
Radvision	IP/VC Gateway
Rapid7	NeXpose Security Scanner
Redhat	Linux
Redhat	Enterprise Linux

<b><u>Vendor</u></b>	<b><u>Model</u></b>
NSFOCUS	NIDS
Nutanix	Controller VM
OKTA.com	OKTA
OpenBSD	OpenBSD
OpenSuSE	Linux
Oracle	Database Server
Oracle	MySQL
Oracle	WebLogic App Server
Oracle	Acme Packet Controller
Palo Alto	PAN-OS
Panasonic Aero	Broadband Controller
Panasonic Aero	Network Controller
Panasonic Aero	File Server

<b><u>Vendor</u></b>	<b><u>Model</u></b>
Redhat	JBOSS App Server 5.x
Redhat	JBOSS App Server 6.x
Redhat	JBOSS App Server
RIM	BlackBerry
Riverbed	Steelhead
Ruckus	SmartOS WLAN AP
Ruckus	SmartOS WLAN Controller
Salesforce	Salesforce Audit
Samsung	Ubigate
SangFor	VPN
SCO	Unixware
SCO	OpenServer
Sendmail.org	Sendmail Mail Server

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>SGI</b>	Irix
<b>Sharp</b>	AR
<b>Slackware</b>	Linux
<b>Snort-org</b>	Snort IPS
<b>Sonicwall</b>	SonicOS
<b>Sonicwall</b>	Global Security Manager
<b>Sonicwall</b>	Aventail VPN
<b>Sophos</b>	Sophos Endpoint Control
<b>Sophos</b>	Email Gateway
<b>Sophos</b>	UTM
<b>Sophos</b>	Web Filter
<b>Sourcefire</b>	Sourcefire3D IPS
<b>Sourcefire</b>	DefenseCenter
<b>SourceFire</b>	NetworkAMP
<b>Squid-cache-org</b>	Squid Web Proxy
<b>SSH Comm Security</b>	CryptoAuditor

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>TrendMicro</b>	IDF
<b>TrendMicro</b>	Deep Security Manager
<b>Tripp Lite</b>	UPS
<b>Trustix</b>	SecureLinux
<b>Tufin</b>	SecureTrack
<b>Tumbleweed</b>	MailGate
<b>TurboLinux</b>	TurboLinux
<b>Ubuntu</b>	Linux
<b>Untangle</b>	Untangle Security Gateway
<b>Vasco</b>	DigiPass
<b>VMware</b>	Generic
<b>VMware</b>	ESX Server
<b>VMware</b>	ESXi Server
<b>VMware</b>	vCNS Manager
<b>VMware</b>	vShield
<b>WatchGuard</b>	Firebox

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>Sun</b>	Solaris
<b>SUN</b>	Glassfish App Server
<b>Sun</b>	SunOS
<b>SuSE</b>	Linux
<b>Symantec</b>	Manhunt Network Security
<b>Symantec</b>	Endpoint Protection Service
<b>Symantec</b>	Data Loss Prevention
<b>Tektronix</b>	Phaser
<b>Tenable</b>	Nessus Security Scanner
<b>Tenable</b>	Nessus6 Security Scanner
<b>Topsec</b>	TOS
<b>Toshiba</b>	eStudio
<b>TrendMicro</b>	Antivirus Manager

<b><u>Vendor</u></b>	<b><u>Model</u></b>
<b>WatchGuard</b>	System Manager
<b>Websense</b>	Web Security
<b>Websense</b>	Mail Security
<b>Websense</b>	Log Server
<b>WindRiver</b>	BSD OS
<b>WindRiver</b>	VxWorks
<b>Xerox</b>	Phaser
<b>YXLink</b>	Vuln Scanner
<b>Zenith Infotech</b>	Zenith ARCA