

## What is SIEM?

Incorporating a Security Information and Event Management (SIEM) device into a *DisPatch* solution provides real-time access to crucial information throughout a network. By aggregating data from firewalls, applications, databases, servers/hosts, and other third-party sources, the SIEM delivers large quantities of data from a single interface, saving administrators time to manually compile the information. FoxGuard's SIEM is easy to use, has extensive reporting capabilities, and is supported by a very responsive technical team.



## Features:

- ▶ Presents network and system data using graphical dashboards
- ▶ Determines potential threats based on correlated data
- ▶ Analyzes data for forensics and incident response
- ▶ Stores log files with signatures for compliance
- ▶ Automatically calculates baselines to analyze trends and detect anomalies
- ▶ Tracks attack vectors through event/flow correlation
- ▶ Option to detach USBs or restrict usage

## Benefits:

- ▶ Simplifies log aggregation
- ▶ Instantaneously detects incidents through automated log file parsing
- ▶ Speeds forensic and incident reporting
- ▶ Adds a layer of security to the network

### Supports top tier manufacturers:

- |               |              |
|---------------|--------------|
| ▶ 3Com        | ▶ Nokia      |
| ▶ Apache      | ▶ Oracle     |
| ▶ Astaro      | ▶ Redhat     |
| ▶ Barracuda   | ▶ RSA        |
| ▶ Check Point | ▶ SonicWALL  |
| ▶ Cisco       | ▶ SourceFire |
| ▶ Citrix      | ▶ Sun        |
| ▶ Fortinet    | ▶ Symantec   |
| ▶ HP          | ▶ Trend      |
| ▶ Juniper     | ▶ VMWare     |
| ▶ McAfee      | ▶ WebSense   |
| ▶ Microsoft   | ▶ Watchguard |

### in these categories:

- |             |                            |
|-------------|----------------------------|
| ▶ Firewalls | ▶ DLP                      |
| ▶ Routers   | ▶ NAC                      |
| ▶ Switches  | ▶ DAM                      |
| ▶ IDS       | ▶ OS                       |
| ▶ IPS       | ▶ Web & Content Management |
| ▶ AV        | ▶ NTP Servers              |
| ▶ IAM       |                            |



2011.07.01