

THE SOC IN A BOX

CyFlare has packaged a next generation breach detection platform with a 24x7 staffed Security Operations Center.



Deployment Options

100 Series Hardware Appliance

- Remotely monitored and managed appliance including system updates and performance monitoring
- 24x7 Technical Support
- Next day replacement included
- Shipped pre-configured
- Inspect up to 3gpbs network throughput



Virtual Appliance

The sensor can be deployed as an agent, container, virtual or Physical appliance on standard x86 architecture. The software packaging comes in the form of an RPM, DEB, OVA, QCOW2, VHD, AMI or container that can be deployed onto the server or inside VMware, KVM or as a Docker.



SOC Service Benefits

- 100% USA Based SOC Resources within our physical SOC
- No limit on time for incident response investigation
- Dedicated Technical Account Manager (TAM) Included
- Customizable Monthly Security Briefing Report & Call with your TAM
- Deployable SOC within minutes
- Integrates with your current networking and security tools
- No per software agent / sensor fees
- Month to Month Contract term available
- 24x7x365 Proactive Monitoring & Investigation
- No Fees to add/change/delete network devices or servers

Security Platform Features

- Artificial Intelligence / Machine Learning based. Both Supervised & Un-Supervised learning
- File Sandboxing - 0 Day Threat Detection
- Shadow IT Identification
- Integrated SIEM
- Best of Breed Threat Intelligence Feeds
- Malware Detection
- DNS Tunnel Detection
- Authentication Monitoring
- Exploit Detection
- Data Ex-Filtration & PII Detection
- Anomalous Traffic Detection
- Anomalous Command Detection
- Anomalous Process Detection
- Command & Control Detection
- Port Scan / Syn Flood Detection
- DGA Detection (Auto-generated domains)
- Cyber Kill Chain Alignment
- Breach Visualization
- Network Traffic Analytics