

Cymphonix Network Composer™

- FULL VISIBILITY AND CONTROL OF INTERNET CONTENT AND APPLICATIONS TO ELIMINATE INTERFERENCE FROM NON MISSION-CRITICAL ACTIVITIES
- URL CONTENT AND APPLICATION BANDWIDTH CONTROLS THAT ALLOW PRIORITIZATION FOR CRITICAL ACTIVITIES
- ROBUST MALWARE DETECTION COMBINED WITH TRACKING AND REPORTING OF INFECTED COMPUTERS, INCREASING PROTECTION AGAINST WEB THREATS
- EXTENSIVE PROTECTION AUTOMATICALLY BLOCKS ANONYMOUS PROXIES AND FILTER AVOIDANCE SITES

Network Composer is a deep packet inspection solution that supplies small to medium-sized business with the ability to completely control not only what its users are viewing on the Internet, but which applications are being used. It includes customizable content controls and filters for individual users and groups. Administrators can utilize the integrated, precise reporting to obtain enhanced visibility of Internet traffic; users Internet activities can be monitored in real-time. By applying the dynamic bandwidth tools, limit available bandwidth on less important programs; allocate resources to essential activities in order to achieve optimal productivity.

This complete, Internet usage control protects the network from threat sources, decreasing risk of harm and downtime. Filter avoidance sites are updated hourly, and extensive content analysis identifies and blocks dangerous anonymous proxies. Client ActiveX removal tools are used to cure infected PCs once the malware has been detected, tracked, and reported.

How Network Composer Works

Network Composer is inserted between your firewall and network switches. There are several products that are specific for various Internet speeds and network interfaces, and each are fully loaded to identify and control Internet traffic. Automatic updates are received at its Internet-based management console; alerts and messages may also be distributed electronically with Network Composer configured to an email server. In the event of power failure, network traffic will be allowed to pass through via a fail-to-wire bypass system.



Work Smart: Control and Protect Your Network

- **Protect your network from sophisticated and hidden threats by employing advanced capabilities to scan, identify, and monitor HTTPS traffic**
- **Strong detection and cessation capabilities of malware with four different tools: class ID, URL, MD5 Sum, and non port 80 transmissions**
- **Prevent spyware from reporting back to its central source, reducing the risk of re-infection**
- **Access reports detailing user activity, application traffic, and potential Internet threats**
- **Monitor application and web traffic to set bandwidth requirements and smart priorities/limits to maintain a fast and productive climate for your organization**
- **Reserve resources by blocking non-essential applications such as P2Ps**
- **Gain the ability to monitor the frequency and content of instant message conversations**

Contact WorkSmart for more information by emailing sales@worksmart.com or calling 800-484-1012