



*What is network intrusion detection?*

Network intrusion detection involves the constant monitoring of network traffic for potential misuse, suspicious activity, or security policy violations. Upon recognizing a pattern of misuse, such as suspicious or unauthorized activity, the system automatically responds in a customer-defined manner.

*I have (am purchasing) a firewall, does CyberCop replace my firewall?*

CyberCop is not a replacement for a firewall, but rather a complimentary technology that offers real-time detection and notification when intrusions are occurring. Firewalls were designed to keep outsiders out of network and are good for this purpose. Just like you would have a fence around your property to keep out trespassers, the firewall is the first line of defense from external attack. Intrusion detection is the burglar alarm and motion detectors located throughout your house.

*Do I need to reconfigure my network to use CyberCop?*

No, CyberCop was designed to attach to your existing network. It works without restricting network flow, regardless of the traffic type.

*Do I have to punch holes in my firewall or enable special protocol services to allow CyberCop to operate?*

No, CyberCop communication occurs through existing TCP/IP ports through which most firewalls pass traffic.

*I have a switched environment, how can CyberCop see all of the traffic on a switched link?*

The primary solution is to use the management ports on the switch to 'mirror' information moving to a device to a CyberCop Sensor. The types of devices that should be 'mirrored' are critical hosts, routers, gateways, and support processes such as DNS or NFS servers. CyberCop, like Distributed Sniffer Servers, is most effective in locations where traffic 'pinches' going in and out of routers, firewalls, and key servers.

*What types of misuse activities does CyberCop detect?*

The CyberCop intrusion detection uses signature recognition, which recognizes evidence of misuse in the header or data portion of the packet. The signatures are sophisticated enough to detect attacks that occur over multiple packets, whether the offending information is located in the headers or data portion of the packets. CyberCop can also be configured to recognize critical information specific to that portion of the network, particular device or specific application with user-definable signatures.

*I have never known Network General for Security, why are you in this market, and what is your credibility?*

Network General Sniffer Analyzers have been used by network managers to catch intruders—CyberCop is a technology to automate this process. NGC has teamed up with the WheelGroup Corporation of San Antonio, Texas which is the leading supplier of Intrusion Detection technology to develop CyberCop.

WheelGroup is providing a piece of the CyberCop technology as well as providing Security Consulting Services that you can purchase through Network General. WheelGroup has extensive experience in Information Warfare and were featured in the February 1997 Cover article in Fortune Magazine.

*If WheelGroup has an intrusion detection product, why should I purchase it from Network General?*

CyberCop is a different product from the WheelGroup NetRanger product. Both have their strengths—NetRanger is a perimeter intrusion detection product that uses a firewall router to detect and block intruders. CyberCop is an internal network intrusion detection system that can be deployed within a corporate network. Both products use the same set of intrusion detection signatures to detect attacks.

*I would like to put this on my backbones 100Mb Ethernet, FDDI and ATM, do you have a Sensor for these topologies?*

This will be in the next major release—within 6 to 9 months after CyberCop first ships. Just as Sniffer Analyzers and Distributed Sniffer cover the primary data communications topologies, making CyberCop available on these topologies is our immediate goal.

*How do you know where to deploy the sensors and configure them?*

We built that into the product as an ease-of-use feature. CyberCop Sensors have multiple pre-configured profiles to protect common vital subnets or resources on the network. This eliminates trying to guess what attacks or intrusions might be common in a particular area of the network. It is simple as clicking on the Sensor profile that best matches the location or the device that you want to protect.

*Does the CyberCop System work with an enterprise network management system?*

Yes. CyberCop Alarms can be forwarded to HP OpenView and other management systems that can receive SNMP traps.

*How will an IS operator know when an attack takes place?*

CyberCop is an intelligent response system. Rather than wait for an event to happen while viewing a console, CyberCop alarms the operator through several different methods, such as pager, email, or SNMP message to a Management System. From this alarm, the operator can then view the CyberCop User Interface to gain information on the attack and take corrective action.

*Does CyberCop send back a message or attack to an intruder?*

No. CyberCop captures information on the origin of the attack including source and destination addresses, and type of attack. CyberCop can also start a Trace file that follows the ‘footsteps’ of the intruder. In addition, CyberCop can be configured to drop certain suspicious network sessions, but CyberCop does not have offensive response capabilities. Network General can provide some useful information, both operational and legal on how to respond or eliminate network intruders.

*How do I respond to an attack?*

That depends on the security policy that your organization has in place. There are several ways to respond—watch the attacker and try to determine where they are going and what they are after. If the attack is coming from inside, you can go to the attacker’s physical station and determine if it is a true insider or a spoof. Another method of response is to eliminate the attacker from the network by figuring out the entry point and denying access. For example, if an attacker is coming from ISP X, you can configure your routers to reject all traffic from that network. The most drastic response is to completely remove the entity under attack from the network. This means pulling the plug on a device that is being threatened—usually a host. This is the safest way to combat the threat while isolating damage. This can be done with system administration techniques to make it appear to users and attackers that the host is coming off-line for standard maintenance.