

VANGUARD™ Product Line



The VANGUARD™ line of products are the industry's most advanced devices for detecting and preventing physical cyber attacks on critical network infrastructure.

VANGUARD Models



VANGUARD™ Monitors two or more dark (spare, unused) fibers within the optical cables carrying the critical data. VANGUARD supports standard single-mode or multimode fiber optic cables and can be used to secure existing fiber optic cables. Using patented hub and spoke technology, a single VANGUARD utilizing one rack space can monitor up to eight continuous optical circuits (zones), providing protection for multiple remote buildings or many dozens of user drops per zone in a facility.

OPTIONS:

VANGUARD+Plus™ monitors active (live, data transmitting) fibers in cases where no dark data fibers are available. Please call or visit our website for details.

VANGUARD™ Aerial optimized for aerial outside plant deployments.



VANGUARD™ CS is a bundled solution consisting of the VANGUARD and CyberSecure Infrastructure Management System. VANGUARD CS provides a complete end-to-end cyber security solution including the ability to manage live monitoring and perform immediate alarm dispatching from a centrally managed location.

VANGUARD CS differs from VANGUARD with specialized firmware and hardware components such as 100BASE-T Ethernet connections on the front panel and a unidirectional simplex optical communications port for reporting alarms to an external device.

OPTIONS:

The **StopLight™ Optical Interface** is a remotely configurable fiber optic panel, which interfaces with the VANGUARD CS to shut off data in alarmed zones and limit access to critical information during an intrusion attempt while continuing to monitor the network.

VANGUARD™ and VANGUARD™ CS are available with front or rear optical connection capability. Multimode VANGUARDs support desensitized lead in cables.



CyberSecure IMS Software



CyberSecure Infrastructure Management System™ (IMS) is a software application that works with NIS optical monitoring products to enable centrally managed, live monitoring of critical network infrastructure from anywhere in the world providing first responders with an early warning, affording them time to act and greater potential to prevent damage or theft of data. A unique benefit of the IMS solution called **Fiber Forensics™**, provides investigators with critical information to assist in profiling methods of attack, helping to prevent future attacks.

Manhole Protection System™



The **Manhole Protection System™ (MPS)** continuously monitors the position of manhole and handhole covers and immediately reports a change at any cover. Thousands of covers may be monitored simultaneously if desired, and every cover is individually identified and mapped. Individual identification allows exact location of any attempt to access underground communication systems through a manhole and/or handhole on which a sensor has been installed, and facilitates an immediate focused response by security or law enforcement personnel via the CyberSecure IMS™ Infrastructure Management software application. MPS™ sensors contain no electronic components, require no electrical power, and emit no signals. Because no electricity is involved at any MPS™ sensor location, the sensors are intrinsically safe under all conditions.

OPTIONS:

The **Manhole Protection System™ (MPS) Sensors** utilize a single strand of standard single-mode fiber (SMF) and are inherently immune to electromagnetic and radio frequency interference, emit no signals, and cannot be bypassed without detection. MPS sensors are environmentally rugged, with an IP66 industrial standard package configuration, and may be integrated into virtually any manhole and/or handhole. MPS sensors are designed for the varying environmental conditions often found in manholes and handholes.

The **Manhole Protection System™ (MPS) Controller** connects the sensors using SMF-28 fiber to/from each group of MPST™ sensors (up to 16 channels, each comprised of up to 35 sensors). The MPST™ controllers come in 8-Channel (250+ sensors) and 16-Channel (500+ sensors) models.

