





NetworkIntegrity
SYSTEMS

We Bring Security To Light™

CREATING A COMPLETE SPHERE OF PROTECTION.

PROACTIVE PROTECTION THROUGH OPTICAL SENSING FOR THE INFORMATION, INFRASTRUCTURE, AND CRITICAL ASSETS THAT KEEP ORGANIZATIONS RUNNING

CORPORATE CAPABILITIES BROCHURE

COMPANY OVERVIEW

Network Integrity Systems (NIS) is an advanced threat-detection company.

Using optical sensing technology, our solutions continuously monitor communications pathways, perimeters, boundaries, access points, and critical assets for threats traditional security and network-monitoring systems often cannot see. By detecting tampering, intrusion, excavation, temperature changes, and unauthorized sensing as they occur, and intelligently validating, correlating, and alarming on those detections, NIS enables organizations to respond proactively, before information is stolen, communications are disrupted, assets are damaged, or emerging threats become serious incidents.

TESTED IN THE REAL WORLD

BUILT TO VALIDATE CUSTOMER SCENARIOS

At NIS' Research and Demonstration Facility, visitors from around the world see our solutions in action and test their products alongside them. In realistic environments, we test customer-specific infrastructure configurations and threat scenarios, showing how detections become actionable alarms.



REAL-WORLD CONDITIONS

Test with representative routes, facilities, and installation configurations.

CUSTOMER-RELEVANT THREATS

Test and validate the activities and events that matter to each application.

DEMONSTRATED RESPONSE

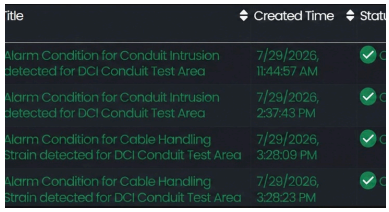
See how sensing, alarm validation, and event management work together.

DATA CENTER INTERCONNECT (DCI) DAMAGE PREVENTION: A RECENT EXAMPLE

Working with leading optical-cable and conduit manufacturers, NIS evaluated VANGUARD FOCUS™ across 50- and 100-kilometer fiber routes. Testing under representative installation conditions demonstrated detection and alarming for manual digging, excavation activity, conduit impacts, and cable handling in manholes. The work shows how continuous sensing can give operators awareness of threats to a DCI route from installation through ongoing operation.









THE NIS SPHERE OF PROTECTION

01 PROTECT THE INFORMATION

Fiber carries an organization's most sensitive information. NIS detects network tampering, intrusion attempts, and fiber-based eavesdropping, helping prevent information from being stolen and communications from being compromised.

02 PROTECT THE INFRASTRUCTURE

Communications networks often fail physically before they fail digitally. NIS detects excavation, cable damage, tampering, and physical attack along the routes that keep critical operations connected and running.

03 PROTECT THE ASSETS AROUND IT

Perimeters, borders, rooftops, corridors, and access points: optical sensing turns fiber into wide-area awareness, detecting activity before it becomes unauthorized entry, asset damage, or loss.

04 TURN DETECTION INTO ACTION

Detection only matters if operators act on it. NIS validates alarms, correlates events across systems, and gives operators the ability to respond decisively and proactively.

PRODUCTS & CAPABILITIES

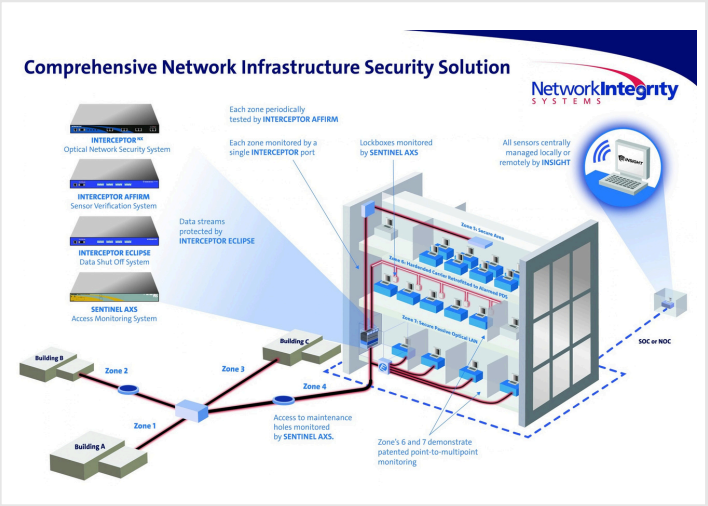
FIVE PRODUCT FAMILIES. ONE SPHERE OF PROTECTION.

NIS applies distributed acoustic sensing, distributed temperature sensing, fiber-access monitoring, and other advanced optical technologies, matching the sensing method to the threat, environment, and mission.

INTERCEPTOR™

U.S. CLASSIFIED NETWORK PROTECTION

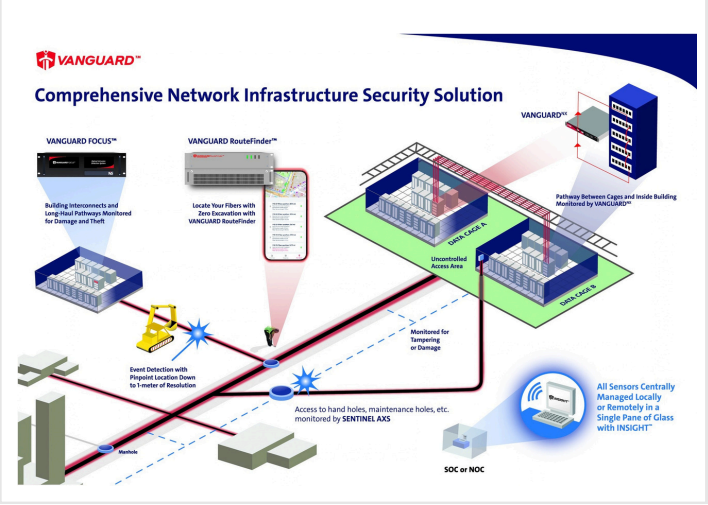
The INTERCEPTOR™ product family protects classified and mission-critical communications by continuously monitoring network pathways for physical intrusion, tampering, and disruption. Its capabilities include Alarmed Protected Distribution System (PDS) in compliance with CNSSI 7003 for secure facilities, long-range distributed sensing, automated system verification, and rapid data shutoff, helping US government, military organizations and defense contractors prevent information theft, protect network availability, and respond immediately to physical threats.



VANGUARD™

ENTERPRISE & CRITICAL-INFRASTRUCTURE NETWORK PROTECTION

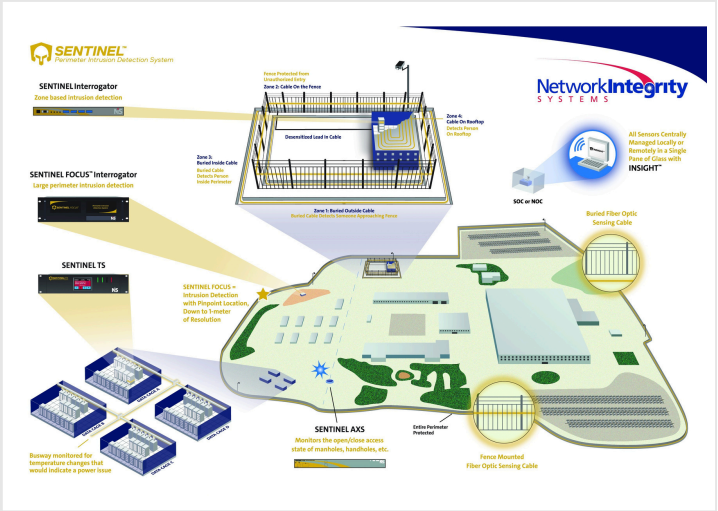
The VANGUARD™ product family protects enterprise, data-center, telecommunications, and critical-infrastructure networks from physical attack and service disruption. Combining cable location, continuous monitoring, and long-range distributed sensing, VANGUARD helps operators locate fiber routes and detect and pinpoint tampering, intrusion, excavation, cable damage, and other activity that could compromise data or interrupt communications.



SENTINEL™

PERIMETER, BOUNDARY & ASSET PROTECTION

The SENTINEL™ product family provides comprehensive protection for perimeters, boundaries, facilities, and critical assets. Its fiber optic sensing capabilities detect fence cutting and climbing, tunneling, foot and vehicle activity, access into manholes and cabinets, and temperature-related threats. This delivers wide-area situational awareness across fence lines, rooftops, open ground, buried pathways, access points, and linear infrastructure.



INSIGHT™

UNIFIED ALARM MANAGEMENT PLATFORM

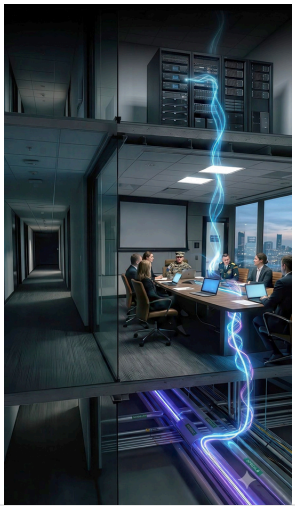
INSIGHT™ brings NIS' fiber optic sensors and the security systems around them into a unified operational view. It correlates related detected events and provides alerts and notifications, helping security operators initiate the appropriate response, while creating an audit trail of events and actions taken.



INLIGHTEN™ NEW

EAVESDROPPING DETECTION

InLighten™ detects attempts to exploit fiber, including dark fiber, as an unauthorized microphone, a threat known as Eavesdropping over Fiber (EoF). Conversations can be captured without accessing network equipment or placing a detectable listening device inside the secure space, allowing an adversary to listen from kilometers away. InLighten provides patented, real-time detection, raising the alarm before sensitive information is compromised.



INTELLIGENT ALARM MANAGEMENT

Cameras and access-control systems show what happens at known points. NIS extends detection across the spaces between them, along network routes, boundaries, fence lines, buried assets, and rooftops. INSIGHT™ integrates NIS optical sensors with video management systems and other intrusion detection devices, turning raw detection into validated, actionable events.

DETECT

Optical sensors detect activity across critical spaces and ancillary security systems feed one platform.

VALIDATE

Detected events are evaluated using correlated sensor data, while using video management system footage for confirmation.

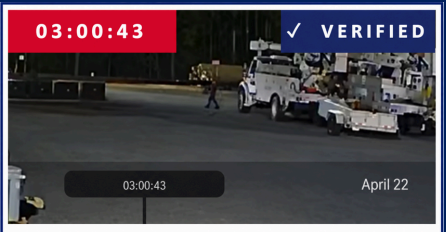
CORRELATE

Related events across systems combine into a single threat picture.

ACT.

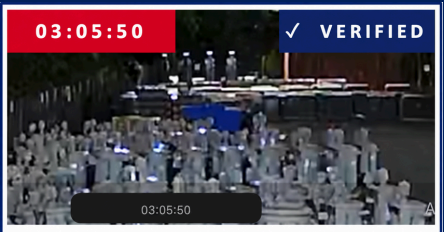
Response workflows, notifications, reporting, and system integrations help operators take decisive action from a single pane of glass.

WHAT SENTINEL™ DETECTED BEYOND CAMERA COVERAGE



INSIDE THE PERIMETER

Person walking the equipment yard near utility trucks.



EXITING OVER THE FENCE

Climbing the fence to exit. Caught by fiber, not cameras.



PINPOINTED ON THE MAP

INSIGHT dashboard showing fiber-sensed intrusion points and path of travel.

DETECTION IN ACTION

At a critical-infrastructure site, NIS detected an intruder climbing the perimeter three separate times in an area missed by existing cameras, enabling operators to activate additional security resources and respond with confidence.

WHAT WE DETECT



NETWORK DAMAGE, CUTS AND THEFT



UNAUTHORIZED EXCAVATION



PERIMETER & BOUNDARY INTRUSION



ROOFTOP INTRUDER DETECTION



SERVICE DISRUPTION



UNAUTHORIZED ACCESS



TEMPERATURE ANOMALIES



FIBER-BASED EAVESDROPPING

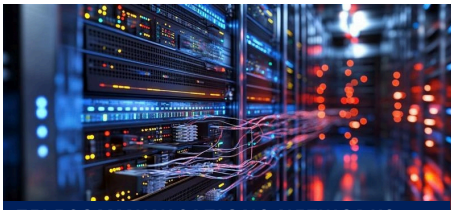
WHERE WE PROTECT



GOVERNMENT & MILITARY



UTILITIES



TELECOMMUNICATIONS NETWORKS



DATA CENTERS & DCI NETWORKS



INDUSTRIAL



BORDERS

THE NIS ADVANTAGE: DETECT EARLIER. RESPOND SMARTER.

DETECT EARLIER

Identify tampering, intrusion, excavation, and other threats as they happen, giving teams time to act before damage or disruption occurs.

COVER THE GAPS

Monitor fiber routes, fence lines, buried pathways, rooftops, and access points where cameras and conventional sensors have limited reach.

VERIFY THE THREAT

Pinpoint where activity occurs and cue integrated cameras or other security systems to help operators see what triggered the alarm.

TURN DETECTION INTO ACTION

Validate and correlate alarms, guide the appropriate response, and create an audit trail of events and actions taken.

Pentagon photograph: U.S. Air Force, via DVIDS. The appearance of U.S. Department of War (DoW) visual information does not imply or constitute DoW endorsement.

Network Integrity SYSTEMS

Since 2003

FOUNDED TO MEET A PENTAGON REQUIREMENT

NIS was founded in 2003 in North Carolina, when optical engineers from a global fiber optics leader answered a DoD requirement to better protect secure fiber networks in and around the Pentagon. Since then, NIS has been granted 50+ patents and has deployed thousands of systems around the globe.

2003	Founded in Conover, NC, to protect classified U.S. government and military networks
2004	INTERCEPTOR™ began its adoption across the Department of Defense, federal government and Intelligence Community
2009	Point-to-multipoint patent granted, reducing hardware requirements and costs while expanding coverage
2014	VANGUARD™ launched for commercial, foreign government and international defense networks
2016	Network protection deployed across a global cloud service provider's data centers and critical interconnect infrastructure.
2018	NIS Services team launched; FOCUS Distributed Acoustic Sensing technology introduced; SENTINEL™ Perimeter Intrusion Detection System launched
2023	Next-generation INTERCEPTOR NX launched
2024	Next-generation FOCUS platform launched; INSIGHT™ intelligent alarm management platform introduced; SENTINEL TS Distributed Temperature Sensing launched
2025	ECLIPSE automated data shutoff solution launched; AFFIRM automated sensor verification solution launched
2026	SENTINEL AXS and InLighten™ introduced; expanded long-distance DCI testing validated proactive fiber-route protection at up to 100 kilometers.

NIS-CONTROLLED EXPERTISE

Today, from inception to completion, NIS designs, manufactures, installs, provisions, and services its solutions.

- **U.S.-BASED DESIGN, ENGINEERING & SUPPORT**
- **CLEARED PERSONNEL FOR CLASSIFIED DEPLOYMENT AND SUPPORT**
- **2024 FOSA INNOVATION AWARD, SENTINEL™ BURIED PERIMETER DETECTION**



Let's discuss what may be going undetected in your operations.

Scan to contact NIS

1937 Tate Blvd. SE
Hickory, NC 28602 USA
877.NIS.4PDS (877.647.4737)
www.networkintegritysystems.com