

## CyberSecure IPS CyberSecure Infrastructure Monitoring System (IMS)<sup>™</sup>

### Global Monitoring System for Unified Cyber-Physical Protection<sup>™</sup> (UCP)

The CyberSecure IMS<sup>™</sup> software platform is at the core of the Unified Cyber-Physical Protection<sup>™</sup> (UCP) suite of solutions, providing a single dashboard to pull together multiple product sets designed to protect, defend, and monitor Government and Commercial network infrastructures. Developed to meet the strictest compliance regulations in the DOD space, it has now become a powerful tool in the Government and Commercial sector to protect against Layer-1 and physical intrusion attempts across all industries that have the need to protect critical infrastructure. As we expand our portfolio of solutions, the dynamic nature of the CyberSecure IMS<sup>™</sup> software enables rapid innovation and scalability. Integration with existing security systems, network monitoring solutions,

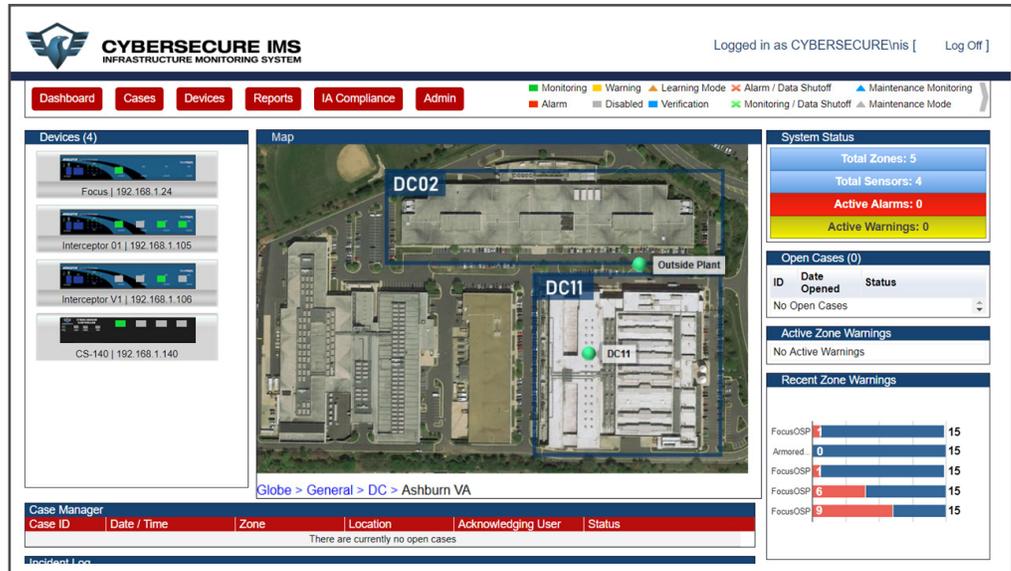
and video surveillance systems are achieved with our APIs. Whether it's IT, OT, or IOT, CyberSecure IMS<sup>™</sup> can provide the single pane of glass to ensure our customer's critical infrastructure protection needs are met.

The CyberSecure IMS<sup>™</sup> 'Rapid Analysis' dashboard gives both Physical Security Officers and Network Security specialists the ability to monitor an entire office building, campus or global network in seconds with easy to use visual tools. The CyberSecure IMS<sup>™</sup> user friendly dashboard helps personnel identify and analyze optical disturbances as they happen and react immediately according to the severity of the incident.

#### System Highlights:

- ▶ First DOD accredited software solution for Infrastructure Cyber Security monitoring
- ▶ Meets the strictest Government compliance standards
- ▶ Central UCP platform to monitor Outside Plant and Inside Plant sensors
- ▶ Distributed architecture allows for global enterprise level deployments

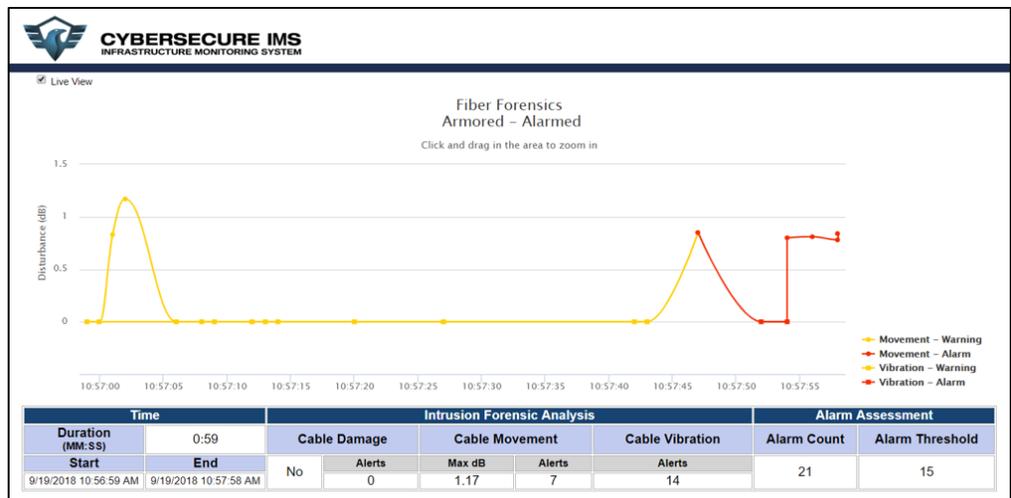
# CyberSecure IMS™ Key Features:



CyberSecure IMS™ Console

## Fiber Forensics™ Intrusion Analysis:

In order to help personnel make informed decisions regarding alarm response protocols, it is important to have a graphical representation of every optical disturbance as it occurs. The CyberSecure IMS™ system contains patented Fiber Forensics™ technology which works in conjunction with the sensors by capturing characteristics of real-time intrusion attempts and displaying it via the IMS™ user interface. With graphical representation of every optical disturbance as it occurs, personnel can use this information to determine immediate and appropriate alarm response including on-site inspection. Optical signatures are tracked depending on the severity and provides valuable intelligence including time stamp, dB loss, number of occurrences, and the duration of the event.



Fiber Forensics™ Display

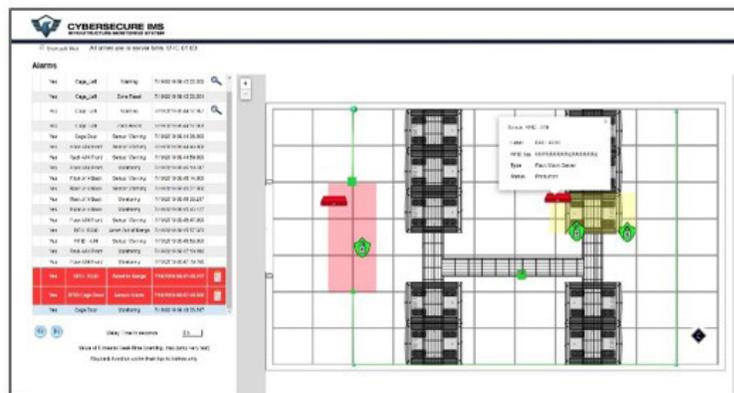


## Optical Intrusion Warning System™

Our patented Optical Intrusion Warning System™ gives personnel the information necessary to reduce the number of nuisance alarms by as much as 99%. CyberSecure IMS™ gathers unique optical signature information from the hardware devices every time an optical disturbance is detected on an alarmed cable and analyzes the severity of the event. With CyberSecure IMS™, personnel are now armed with real-time information that allow them to distinguish between accidental contact disturbances and real intrusion attempts. Furthermore, they can create user configurable warning thresholds per zone. The warning system replaces the antiquated relay-based alarm systems with an intelligent interface that only triggers the alarm when the threshold is crossed.

## Just Press Play™ (JPP) - Rapid Troubleshooting Feature

This rapid troubleshooting feature is akin to having a “DVR-like” capability that significantly reduces the time needed to troubleshoot or investigate an outage or incident. Since CyberSecure IMS™ logs and stores every warning or alarm that is triggered, administrators can go to any point in time to play back the events that occurred on the console viewer. JPP’s ability to visualize events and correlate the data is critical to any incident review or post-mortem activity. Armed with this data, security teams can determine the underlying cause within their network infrastructure in seconds allowing for remediation protocols to begin immediately.



Just Press Play™ Display

## Case Management with Integrated SOPs & Automated Reports

Every alarm triggers a new case with a unique ID number that is logged. Each case remains open and the incident is kept in an alarmed state until required steps are followed. These remediation procedures and case management is completely customizable within CyberSecure IMS™ according to the customer’s needs.

- ▶ Receive daily, weekly, monthly, quarterly and/or yearly Health Reports regarding the activity occurring in the environment on a zone by zone basis.
- ▶ Provide the SOC team with the ability to analyze trends in the network which often leads to the prevention of nuisance alarms before they occur and help admins proactively recalibrate the alarmed zones when site conditions change.



## Integrated Alarm Dispatching

The CyberSecure IMS™ software provides constant monitoring of every cable, zone, building and campus for warnings and alarms. Real-time alerts are displayed on the console and can be sent via email, text, or call out to a voice dialer via dry contact to ensure that the appropriate security personnel are immediately notified of an incident. More important, CyberSecure IMS™ includes features to provide visual guides in the facility to the area affected so that security personnel know where to go. Alarm response teams are equipped with zone-specific information through the IMS™ software via:

- ▶ CAD Drawings
- ▶ Standard Operating Procedures
- ▶ Combinations to Locks
- ▶ Digital Images
- ▶ Special Instructions
- ▶ Video Footage

## CyberSecure IMS Zonar with Eagle Eye Active Intruder Alert System™

- ▶ The Eagle-Eye Security Sensor allows the dispatch center to provide additional intrusion warnings for first response personnel to identify on-going attacks before they arrive in the danger zone.
- ▶ The remote capabilities of the Zonar Security Sensor help keep first responders safe by providing them with a real-time visual indicator of all intrusion attempts while completing their investigation using a smart phone or tablet.
- ▶ Upload images of damaged or missing cables to the CyberSecure IMS™ server during an investigation.

## Ease of Integration with existing/legacy systems.

CyberSecure IMS™ has dynamic API capability for seamless integration with existing/legacy security systems that may exist in customer environments. This provides for both Northbound and Southbound integration with commercial security systems such as Lenel or Government systems such as Vindicator. In addition, CyberSecure IMS™ can also integrate with enterprise monitoring platforms such as Solar Winds. Our team of software engineers can work with the customer to ensure that the IMS™ software is integrated seamlessly into the environment to provide convenience and ease of use.

## CyberSecure IPS Custom Solutions

**Not exactly what you're looking for? We work closely with our clients to provide them the best solutions for their needs. Contact us to schedule a meeting or a demo of our solutions.**