

# Endpoint Detection & Response (EDR)

## Overview - The Challenge

As cyberattacks become more sophisticated defending against endpoint-focused attacks has never been more challenging.

Compounding the challenge is the fact that attackers work 24x7, while most organizations IT departments do not. Not to mention, endpoints are commonly overlooked due to the amount of data, applications and connections across environments.

**This exhausts IT members and creates unnecessary risk to most organizations.**

We understand staying current and obtaining the advanced knowledge needed to keep your organization safe from intelligent attackers is difficult. We also understand that retaining staff, especially at this time, is the most challenging it has been in decades!

## How We Do It

InfoSight's team of expert analysts alleviate resource constrained IT teams by providing the expertise and EDR solution needed to defend and respond against any attacks missed at the endpoint and synchronizes all environments into a "single pane of glass" for easy viewing.

Our trusted professionals quickly coordinate remediation support and incident response solutions through patterns and repetition as well as new adjustments for immediate endpoint protection saving your organization time and money.

## Key Service Features

- 24x7 Comprehensive Security Monitoring
- Containment, Mitigation & Remediation
- Incident Response
- Attack Intelligence
- Behavior Monitoring
- Endpoint Policy Creation & Management

# Endpoint Detection & Response (EDR)

## A Deeper Dive into InfoSight's Services



**24x7 Comprehensive Security Monitoring** - InfoSight's SNOC monitors all your assets in the Data Center and the Cloud regardless of data source 24x7x365.



**Containment, Mitigation & Remediation** - Incident response steps are predetermined and applied resulting in successful containment and recovery



**Incident Response** - InfoSight's SNOC Analysts can take action on your behalf to stop attacks, contain incidents and minimize risk.



**Attack Intelligence** - We leverage intelligence resources and threat vectors that are gathered from global sources.



**Behavior Monitoring** - Looking for patterns and similarities in system's behavior along with suspicious activity.



**Endpoint Policy Creation & Management** - Withhold compliance and industry specific standards, ensure your organization is up to date on policies and procedures.

## Why InfoSight

- 24x7x365 US-Based SOC/NOC
- SOC 2 Certified
- Complete MSSP Services that include Monitoring, Real-Time Threat Analysis, Mitigation/Remediation, Alerting, Reporting and Device Management
- Flexible pricing models that can be 24x7, 8x5, or off-peak 7pm to 7am only coverage
- 22+ years Regulatory Compliance experience (GLBA, PCI, HIPAA, NERC, AWWA, etc.)
- Certified Experts (CISSP, CISA, CEH, OSCP, AWS, AWWA, etc.)
- Managed Services for On-premise Data center, Cloud and Hybrid environments