CASE STUDY – CYBIR

# MAGNET IGNITE™

Using Magnet IGNITE to Accelerate Breach Response Cases

> Our customers need these answers as quickly as possible to minimize business interruption and Magnet IGNITE has enabled us to provide them hours—and sometimes days—earlier."
>
> — **Michael Nelson, Managing Partner, CYBIR**

## The Challenge

When a business suffers a breach, they turn to CYBIR to investigate the incident. CYBIR needs to be able to move quickly and gather insights on the breach and determine the course of action required to guide the company through the incident.

With time in short supply, CYBIR needs to identify which endpoints were affected quickly. They also need to provide answers to the business and legal counsel on how the attack occurred and what data was accessed or exfiltrated. To ensure the speed and efficiency of their triage, CYBIR uses Magnet IGNITE, a cloud-based tool that enables concurrent, targeted collections from remote endpoints.

Prior to using IGNITE, a breach required CYBIR to travel to the client site, send drives overnight to and from the client to gather full disk images, or use various scripts to extract data. Between transportation timelines and the volume of data that needed to be processed and investigated, it could take days or weeks to reach the required answers.

With the constantly evolving nature of breach investigations, speed is important not only at the onset of the investigation but also when a development takes the case in an entirely new direction. The efficiency of IGNITE allows CYBIR to deploy additional agents and review evidence at speed—maintaining the momentum and progress of their investigation.

CYBIR

CYBIR is a cybersecurity, digital forensics & incident response consulting firm serving clients across the United States.

**HEADQUARTERS**

- Philadelphia, PA

**SIZE**

- 10 – 25 Employees

**SPECIALTIES**

- Breach Response
- Digital Forensics, eDiscovery, & Data Recovery
- Data Security and Privacy Compliance
- Penetration Testing and Managed Security Services

# How Magnet IGNITE Helps

## Speed and Efficiency

Magnet IGNITE enables the rapid triage of remote client endpoints to identify where malicious activity has taken place so examiners can determine the required next steps. Using a single agent configuration, examiners can triage multiple endpoints at the same time to quickly gather insights into an incident and determine where a full forensic analysis is needed.

## Initial Analysis to Deep Dive Forensics Tools

Triage results are presented in IGNITE's intuitive interface to allow for preliminary analysis of artifacts, as they are being collected. Keyword searches and time filters can be applied to the results to provide many of the answers that are required in data breach cases. Where a deep forensic analysis of an endpoint is required, IGNITE can export evidence in a file format that can be ingested into Magnet AXIOM Cyber.

## Cloud-Based Benefits

With teams and projects geographically spread across multiple states or internationally, IGNITE provides hybrid teams with access to the data no matter where they are located. As a cloud-based tool, IGNITE can be accessed from any location with an internet connection to quickly triage endpoints. And because IGNITE operates completely in the Cloud, it doesn't require processing time or additional hardware in your forensics lab.

> Data breaches can happen anywhere in the world and one of the most powerful features of Magnet IGNITE is that it allows us to investigate how they happened, actions the threat actors took and what data was exfiltrated, from any remote location.
>
> **— Michael Nelson, Managing Partner, CYBIR**

See IGNITE in action for yourself.

To learn more about Magnet IGNITE and get started with a free trial visit magnetforensics.com/magnet-ignite.



MAGNET FORENSICS®