CASE STUDY - FORTIS BY SENTINEL

MAGNET IGNITE™

Fortis Accelerates Endpoint Sweeping by 70%, Initiating the Path to Faster Recovery

> With IGNITE, we conduct very quick and rapid initial triage with endpoint sweeping. Compared to traditional forensics with scripted tools, we see a 70% time savings on data gathering and initial endpoint sweeping.
>
> — **Ted Joffs, National Incident Response Manager, Fortis by Sentinel**

The Challenge

'Slow and Finicky' Tools

As the National Incident Response Manager for Fortis by Sentinel, Ted Joffs is often called into action for people having their worst workday ever. Hit by ransomware or other malware attacks, many business victims are vulnerable and frantic. They need help, fast.

Fortis responds with a team of specialists to counteract the breach. Since conducting deep analysis of every potentially impacted endpoint requires massive amounts of time and money, the forensics provider must first triage the threat. They previously used scripted data collection tools for initial review. However, these products proved lacking.

"Scripted data collection tools tend to be slow and finicky," Joffs notes. "They are often reliant on having the correct tools underneath, depending on the type of platform."

Fortis needed a faster, reliable tool for sweeping endpoints and minimizing the total number of endpoints requiring a deep dive.

FORTIS by Sentinel
Advancing Your Protection

Fortis by Sentinel provides end-to-end protection and recovery that reduces risk and eliminates vulnerabilities

HEADQUARTERS

- Downers Grove, IL

SIZE

- 450+ professionals

SPECIALTIES

- Penetration testing
- Incident response
- Security and compromise assessments

RESULTS

- Eliminates cost and effort tied to extraneous deep-dive forensics
- Contributes to client recovery in half the time of competitors
- Drives development of long-term relationships

How Magnet IGNITE helps

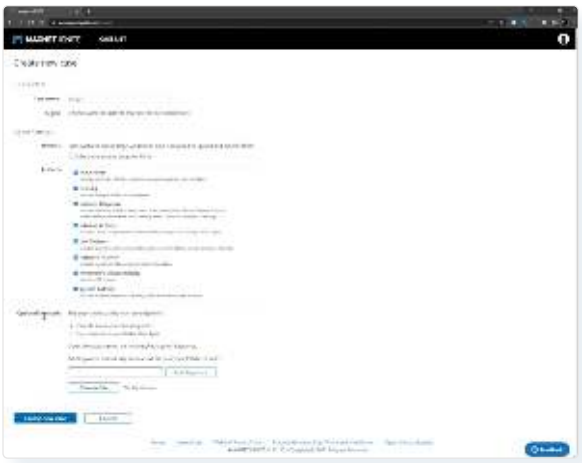
Accelerating Response

As an extensive user of Magnet AXIOM Cyber for investigation, Fortis trusts Magnet Forensics' attention to detail and continuous innovation. The firm then became early adopters of Magnet IGNITE upon the recommendation of a team member who used the triage tool in his previous work.

"Our digital forensics and incident response teams use IGNITE to get fast results ... that eliminate the need for extraneous deep-dive forensics," Joffs says.

In fact, by 'knowing where to dig,' according to Joffs, IGNITE serves as a kickoff to response and recovery that helps clients recover within half the time compared to some competitors.

"Anytime you can speed up the forensics process, you definitely have an advantage," he says. "IGNITE supplies that advantage."



Fast Targeting

In the hands of Fortis specialists, IGNITE ensures skilled time and energy is allotted with speed and precision.

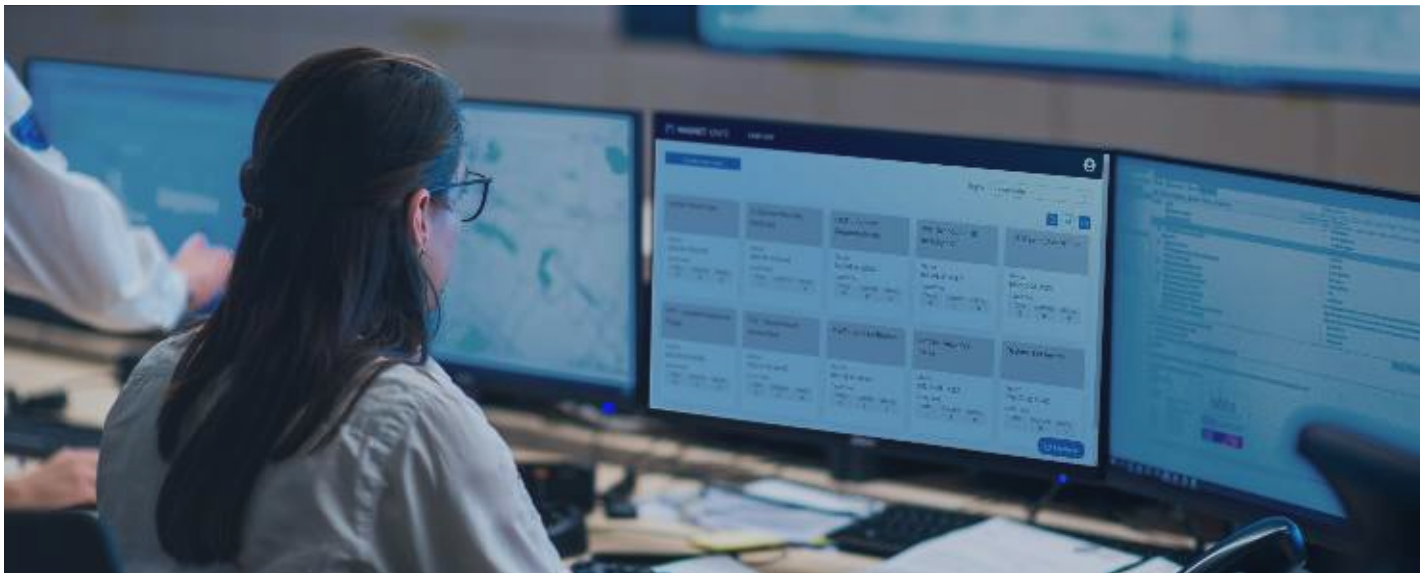
"With IGNITE, we conduct very quick and rapid initial triage with endpoint sweeping," Joffs notes. "Compared to traditional forensics with scripted tools, we see a 70% time savings on data gathering and initial endpoint sweeping."

In Fortis investigations tied to ransomware activity, IGNITE identifies indicators of compromise and threat actor activity faster than previous methods, empowering analysts to sprint with targeted confidence.

> "If we're recovering data from 100 systems and IGNITE quickly identifies that only two of them require a full forensic analysis, we're able to save hours of response time," Joffs says.

Fortis and its customers also save the related cost of deep-dive forensics for unaffected systems, compromised endpoints can be easily exported for investigation with AXIOM Cyber.

"A lot of people take incident response and digital forensics as separate things," Joffs says. "But, when endpoint sweeping ties back into one control, you can quickly identify all assets that have been impacted to limit the scope of recovery and rebuilding."



Cloud-Based Triage

Compared to high maintenance scripted data collection, IGNITE works out of the box to complete fast, remote triage of endpoints. Also, instead of methods that require manual FTP and review, IGNITE enables analysts to review findings immediately. Fortis experts spend their time gathering insights, not configuring tools.

Furthermore, cloud-based triage serves analysts and customers where they are. While the majority of Fortis clients are U.S. corporations, large scale organizations often maintain multiple regional and global offices, with a majority of employees working remotely. The same is true for the Fortis DFIR team guiding customers through response and recovery while managing location- and industry-specific regulations and reporting.

"Everyone is remote now," Joffs relates. "Being able to work remotely and collaboratively is key."

Cloud-based processing also supports scalability–whether high or low volume, all client needs are met, according to Joffs:

"IGNITE scales well because it's talking to the Cloud and has a good infrastructure for ingesting data quickly."

Case-Building and Compliance

Through efficiency, Fortis gains the trust of clients, legal teams, and insurance providers. Analysts rely on IGNITE to target only exposed assets, then they funnel the results to AXIOM Cyber for investigation critical to building a case. "Any time you have an incident case, legal teams want the data as quickly as they can get it," Joffs explains.

> "The speed of collection and providing findings to a legal team is a major competitive advantage."

Up to date with ever-growing requirements, IGNITE and AXIOM reporting capabilities enable Fortis analysts to demonstrate regulatory compliance and understanding of the root cause of an incident. "Magnet solutions give us the capability to build out comprehensive timelines," Joffs notes. "It's really important that we can gather that data and then see it in formats that are easily readable."

The Impact

Client Resilience

Powered with IGNITE remote triage and AXIOM Cyber analysis, Fortis restores organizations to their core missions–whether it's supplying healthcare, protecting investments, or other vital services.

Company Growth

Along with the satisfaction of helping clients resume operations, Joffs and his team foster connections that help Fortis grow. In fact, transactional cases–amounting to almost a third of overall client work–often serve as initial interactions that lead to ongoing partnerships.

> Once you've recovered an environment, you know you've helped a customer through the hardest day of their career," Joffs concludes. "Then, trust comes through and tends to build a long-term relationship."

See Magnet 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®