CASE STUDY - BREADCRUMB CYBERSECURITY

MAGNET AXIOM CYBER™

How a Security Firm Faced BEC, Tripled Caseload Capacity

> For complicated BEC attacks, trying to efficiently unwind malicious parties, domains, and more becomes next to impossible without a tool like AXIOM Cyber."
>
> — **Brian Horton, CEO, Breadcrumb Cybersecurity**

The Challenge

BEC Explodes

It happened fast.

Business email compromise (BEC) attacks overtook ransomware as the top concern for Breadcrumb Cybersecurity and its clients in just a matter of months.

"It's gone through the roof," noted CEO Brian Horton. "For us, BEC is now–by far–the highest caseload and loss per victim." In fact, he said, the attacks hit central California firms 10 times harder than ransomware, with some losses exceeding half a million dollars.

A single case can involve millions of artifact hits across multiple data sources. "We have a working skill set and knowledge but applying that to such a large data set is just staggering," Horton noted.

Also, it's tricky business.

BEC attacks have grown exponentially more complex, involving multiple impersonations and fake threads streaming through at the same time.

Breadcrumb™ CYBERSECURITY

Breadcrumb Cybersecurity helps organizations protect their infrastructure, data, and reputation from advanced cyber threats.

CHALLENGES

- Seeing clients through explosion of costly BEC attacks
- Handling the high volume of investigation data
- Equipping DFIR staff to work efficiently

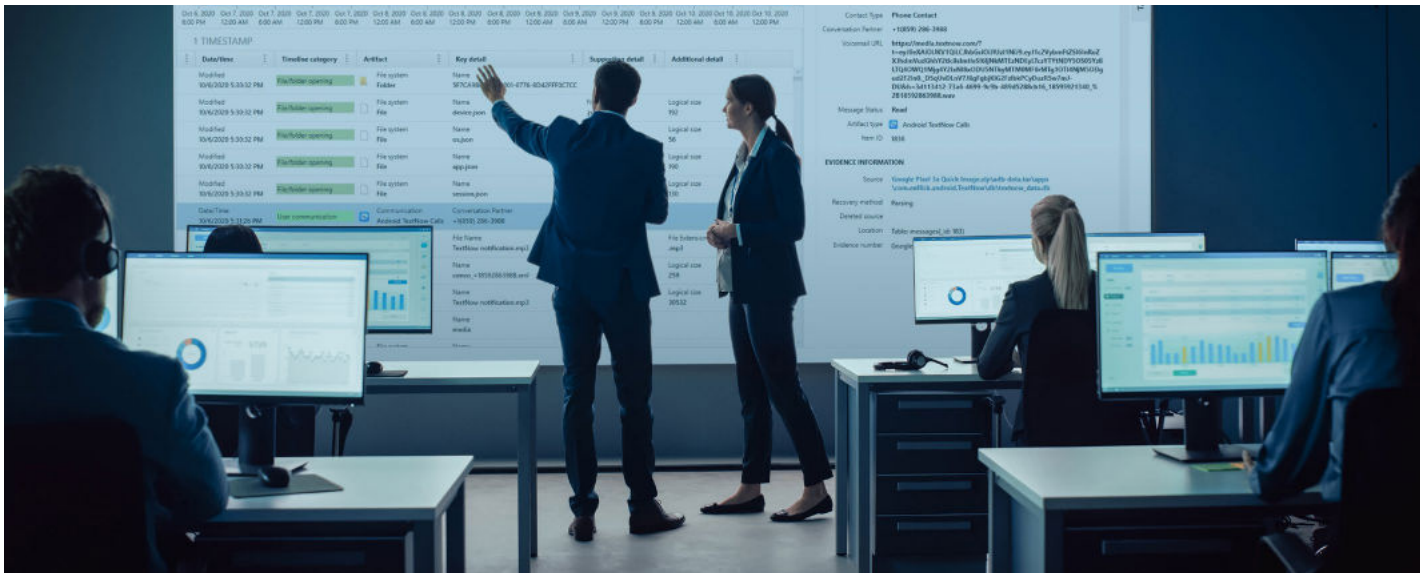
SOLUTION

AXIOM Cyber enables Breadcrumb Cybersecurity to:

- Narrow scope to case-relevant evidence within a day
- Identify connections between extensive artifacts
- Achieve proficiency within a single suite of tools

RESULTS

- Closure of BEC cases in half the time
- Caseload capacity increased by 300%
- Trusted as a problem-solver



Traditional Tools Come Up Short

Before the increase in BEC, Breadcrumb armed its security experts with robust tools to combat ransomware and other cybersecurity threats. Though–from experience–Horton viewed traditional digital forensics and incident response (DFIR) products as short on capabilities and long on training.

While searching for the right tool for his lab, Horton came across a federal agency and local District Attorney's office using Magnet AXIOM Cyber with built-in remote acquisition.

Breadcrumb started a trial.

"Once we imported our first hard drive and cell phone and saw the extensive amount of artifact categories pulled out, I thought, 'Wow, this is incredibly helpful,'" Horton recalled.

2X FASTER
CLOSING CASES

3X CASELOAD
CAPACITY

How Magnet AXIOM Cyber Helps

Reduction Before Rescue

Breadcrumb accelerates the collection and analysis of evidence from computers, the Cloud, and mobile devices with AXIOM Cyber, delivering fast action to combat many types of security threats–even the recent rise of BEC attacks.

> "AXIOM Cyber allows us to reduce content rapidly. In every instance, we can work down to the artifacts relevant to our case within a day."
>
> **– Brian Horton**
> **CEO, Breadcrumb Cybersecurity**

Breadcrumb examiners use Timeline Explorer to narrow the scope of evidence for every case. Then, skilled examiners keep a holistic view by searching keywords, pivoting on timelines, and creating tags to establish their own order of events, a must-have capability to counteract BEC modification by bad actors still in the environment, according to Horton.

When complete, examiners also tag items to create artifact-specific reports that help demonstrate findings to clients: "Then they can see play-by-play what happened and come to the same conclusion that we have."

Examiner Proficiency

Unlike other systems, Breadcrumb examiners find AXIOM Cyber easy to use with intuitive workflows. For instance, a lab analyst–seasoned in law enforcement though new to digital forensics tools–wasted no time getting up to speed.

"Having our analyst go from no experience to product proficiency within three months was a huge plus for us," Horton said.

Scaled Protection

To serve its clients, Breadcrumb needs to manage dozens of cases at once, surfacing relevant details and actionable insights to keep things moving. "With AXIOM Cyber we're pushing through our caseload at scale," Horton said.

Breadcrumb examiners increased the speed with which they import and cull data. "Parsing through artifacts first really helps pare that down," Horton explained. Then, examiners apply their specialized skills to only case-relevant evidence.

"When we're working a case, we're able to reduce content, then go through our process...our time to close is twice as fast," Horton noted. "For BEC attacks, trying to unwind malicious parties, fake domains, and more becomes next to impossible without a tool like Magnet AXIOM Cyber."

For the clients Breadcrumb serves, a shorter turnaround increases their chances of stopping or reversing financial loss and strengthening their position against future attacks.

Increased Caseload

For Breadcrumb itself, ease and efficiency allow the firm to serve more organizations caught in the snare of BEC, ransomware, or other cyber-attacks.

"We can do three times the caseload than we could before," Horton said.

That's triple the opportunities to take down criminals as a trusted problem-solver for insurance companies and managed service providers (MSPs), as well as for organizations with whom Breadcrumb shares a direct relationship.

Also, since the firm offers security operations center (SOC) services, increased capacity feeds directly into another revenue stream. "Pretty much every client that was a victim ends up being a SOC client," Horton said.

Coming full circle, SOC efforts then cycle back to sharpen Breadcrumb's incident response and forensic offering.

"We have a real-world understanding of how other organizations are being targeted and attacked," Horton explained. "So, we take that knowledge and repurpose it for when we work with victims."

> Having our analyst go from no experience to product proficiency within three months was a huge plus for us."
>
> **– Brian Horton**
> **CEO, Breadcrumb Cybersecurity**

See AXIOM Cyber in Action for Yourself

To learn more about AXIOM Cyber and how it can help simplify your forensic investigations, request a free trial at magnetaxiomcyber.com

Or contact us at 1-844-638-7884 or sales@magnetforensics.com to arrange a demo.

MAGNET FORENSICS®