# CASE STUDY:
# Durbin Bennett Tax Advisors

## Tax Firm Takes Preventative Measures to Comply with Pressing Regulatory Obligations and Defend Against Cyber Threats

DURBIN BENNETT

### The Business

- Tax Advisory Firm
- Based in Austin, Texas
- 24 employees (4 remote)
- Faced with impending regulatory pressures and cyber threats

### The eSentire Solution

**eSentire Managed Detection and Response™** employing esNETWORK™ for real-time network threat detection and prevention

## Background

Many small and mid-sized firms consider themselves too small to be targeted by cybercriminals, so they choose to ignore the threat. But, these firms are in fact the easiest targets because they manage highly-sensitive information with limited defenses. If the threat of having their networks and client information compromised isn't urgent enough, the growing number of regulatory obligations should compel smaller firms, especially in the financial services industries, to ensure they have a cybersecurity strategy in place.

## The Challenge

Durbin Bennett Tax Advisors is a 24-person tax firm that focuses on strategic tax consulting, planning, and compliance services. The staff at Durbin Bennett manage their clients' confidential financial information on a daily basis, which makes identity and information security a top priority.

While tax firms are not yet required to follow the same SEC regulations as their counterparts in banking, insurance, brokerage and asset management, Durbin Bennett is experiencing a steady increase in new regulatory requirements from governing bodies like the IRS and the Department of Revenue. Damara Marinello, a project manager who leads cybersecurity initiatives at Durbin Bennett, acknowledges the fact that new regulations are inevitable – especially in smaller segments of an industry that's heavily regulated by the SEC. "The AICPA (American Institute of Certified Public Accountants) is already starting to implement mandates for tax firms," says Marinello. "It's happening every month – there's a new security certification that we know we'll have to comply with."

The firm knew it needed help managing the complexities of the ever-changing regulatory landscape, and protecting their network against threats that could exploit their highly-sensitive client information. Their challenge, however, was that they did not have the necessary time, talent or resources to manage ongoing cybersecurity projects in house. Marinello shared, "We were at a disadvantage because we didn't have an IT person to monitor our network, and we couldn't afford to hire someone at a highly-competitive salary."

**"It's happening every month – there's a new security certification that we know we'll have to comply with."**

esentire

**"We were at a disadvantage because we didn't have an IT person to monitor our network, and we couldn't afford to hire someone at a highly-competitive salary."**

## The Solution

To prepare for the onslaught of new requirements, Durbin Bennett looked to external vendors to help fill the gaps in their cybersecurity approach, looking to their IT partner, ERGOS, for advice about their options. Having worked with eSentire in the past and having experience with traditional cybersecurity technologies and services, ERGOS confidently advised the firm to continue down the path with eSentire Managed Detection and Response™.

Durbin Bennett installed eSentire esNETWORK™, a fully managed, zero-latency IPS/IDS designed for mid-sized organizations. As the primary sensor for eSentire Managed Detection and Response, esNETWORK employs advanced behavior-based anomaly detection and attack pattern analysis to detect and alert on potential threats that have bypassed other security controls. A team of 24x7 security analysts uses highly-sophisticated forensics tools to investigate and respond to odd or suspicious behavior flagged by esNETWORK, and locks it down within seconds.

Now, Durbin Bennett proudly assures current and prospective clients that the safe-keeping of their information is part of their daily operations: "Through multiple layers of web monitoring and security, we have measures in place to help ensure that your personal information is protected," as stated on the firm's website. "With our network security partners, ERGOS Technology Partners and eSentire, Durbin Bennett Tax Advisors is committed to maintaining the security and integrity of all client and firm data. Our network is fully monitored with round-the-clock human oversight to evaluate and eliminate security threats before any potential complications."

## The Results

Durbin Bennett's primary objective for ramping up their cybersecurity was to prepare for impending industry regulations, but they couldn't ignore the real possibility of a business-impacting cyber-attack. And it was a good thing they didn't, because in the spring of 2016, they experienced their first event.

On March 31, eSentire detected adware on an unmanaged PC that was connecting to Durbin Bennett's network. eSentire's Security Operations Centre (SOC) sent an alert to the firm containing recommendations for identifying the threat and mitigating the risk of a breach. With the help of ERGOS, Durbin Bennett investigated the situation and found that the person triggering this alert was a remote user connecting in via remote VPN client. eSentire analysts instructed the client to perform anti-virus and anti-malware scans on the affected machine; verify that anti-virus signatures were up to date; and query the user about their activity to determine whether she intentionally downloaded the software in question.

"The home computer was not managed by the firm and did not have antivirus software installed. It was a total blind spot in their security," a representative from ERGOS stated. "Had eSentire not alerted us, there was nothing else that would have informed us of the situation and the possible threat to the rest of the network."

With the firm's plans to move their operations to the cloud in the coming months, having a comprehensive cybersecurity strategy in place is more important than ever. Ongoing access to trusted experts allows the staff at Durbin Bennett to focus on their clients, rather than worrying about cybersecurity.

## About eSentire

eSentire Managed Detection and Response™ protects firms from constantly evolving cyber-attacks that technology alone cannot prevent. Our 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds to known and unknown threats in real time, before they become business-disrupting events.

esentire

Learn more at **www.eSentire.com**