



## AA Thornton Case Study

Law firms, like many organizations, are susceptible to a range of cyber threats. Given the sensitive nature of the information they handle, such as legal documents, client data, and IP, law firms are attractive targets for cybercriminals. Some of the cyber threats that law firms in particular face: Data Breaches, Phishing Attacks, fileless Malware, Ransomware, APTs, etc. Within their overall cyber defenses, and to counter some of these threats, it is crucial that Law firms implement Endpoint protection solutions, to try and prevent file-based malware attacks, detect malicious activity, and to provide the investigation and remediation capabilities needed to respond to alerts. This is supposed to help law firms minimize potential damage and respond promptly to security incidents.

### The Challenge

AA Thornton's previous endpoint security tool was ineffective in trapping malware, which had exposed their systems to an increased risk of potential security breaches. This shortfall had, in turn, left their organization's valuable and sensitive data in a precarious position, necessitating immediate attention and a more robust solution to fortify their cyber defenses.

### AA Thornton Requirements

Following a major incident, AAT required an endpoint protection solution that would be highly effective in mitigation, would be easy-to-install, and didn't rely on signatures. They also put emphasis on it being straightforward to manage in routine when required by the minimal inhouse IT staff (in terms of ongoing updates and resource requirements), and would not require constant human handling of the dashboard. Given its diverse operating model and remote working policies – AAT also required a Managed Service to replace their existing endpoint protection solution that used a standard signature based AV tool. A market leading EDR tool which they had installed was not proving effective in managing the threats that were targeting the end user devices in addition to the servers.

*"Deceptive Bytes was deployed at AA Thornton via our dedicated UK Partner Hanco, who have been providing security solutions to us for a few years now via their Cybershield service, and with their help we have transformed our security and the threat landscape. We now have an end-to-end endpoint security solution that covers both our servers and endpoints using the Deceptive Bytes product which also provides analytics, metrics, and monitoring by integrating with our SIEM & SOC. Our previous solution was noisy and took significant time looking through alerts and logs to really get to grips with where the threats to our environment lie. Deceptive Bytes solution saves significant time for my team and makes us aware of issues quicker than other solutions we have used..."*

**Vince J. Bixby – IT Manager, AA Thornton**

### Implementation Experience

Hanco expertly managed the implementation at AA Thornton, and the entire process unfolded seamlessly and without any disruptions. What truly set this implementation apart was the remarkable performance of the lightweight Deceptive Bytes agent, combined with the simplicity of the deployment process, which left a lasting impression on all involved.

Industry: Legal Services

Location: London, UK

Headcount: >100

Revenue: £151.4M

### Requirements

- \* Advance endpoint protection
- \* Easy to install and manage
- \* Minimal IT staff to manage

### Solutions

- \* Active Endpoint Deception for Windows
- \* Active Endpoint Deception for Windows Servers

No. Endpoints: 235

### Summary

- \* Quick, simple & seamless deployment
- \* Reduced IT burden
- \* Improved security
- \* Added value to the customer

### About Deceptive Bytes

Deceptive Bytes, a leader in endpoint deception technology, provides its Active Endpoint Deception platform to enterprises & MSSPs which enables them real-time prevention of unknown and sophisticated threats. The solution dynamically responds to threats as they evolve, based on the current detected stage of compromise, and changes their outcome, giving defenders the upper-hand in protecting their assets and data.

Recognized as a [Gartner Cool Vendor](#) in Security Operations and Threat Intelligence.

