



# BLM Protects Employees Against Malicious Email Attachments with Mimecast

**Mimecast Target Threat Protection blocked 121 unsafe attachments and 29 malicious links in just one month, helping to protect law firm's reputation and reducing the risk of disruption to customer service.**

BLM LLP is an insurance and risk law business based in the UK and Ireland. The firm is made up of over 200 partners, more than 800 legal specialists and over 1,700 employees spread across 13 offices.

In common with most organizations today, BLM relies heavily on email as a primary communication tool. IT Technical Operations Manager, Darren Broughton explained:

“Everything we do is by email. We get new instructions by email and we communicate with customers by email, so it's critical to the day to day operation of the business.”

## At a Glance

### Company

- Company: BLM (<http://www.blmlaw.com>)
- Industry: Law
- Number of Email Users: 1,700

### Objectives

- Secure email communications against targeted threats in malicious URLs and attachments
- Protect the firm's reputation by keeping confidential information safe, and preventing disruption to customer service
- Eliminate the significant support burden when employees clicked on suspect links or opened malicious attachments

### Results

- Mimecast Attachment Protect pre-emptively sandboxed 37,000 attachments for deep analysis every week
- Mimecast URL Protect scanned 19,556 links and blocked employees from accessing 29 malicious websites in one month
- Mimecast Targeted Threat Protection eliminates a growing risk exposure, and saves up to 20 support days per targeted threat incident

**“We can be confident that we are thoroughly protecting our employees against targeted attacks in email.”**

*Darren Broughton - IT Technical Operations Manager, BLM*

## Growing Threat

Darren had become increasingly concerned about the risk posed by targeted email attacks, in particular those delivered via malicious URLs and malware-loaded attachments.

He explained: “We’ve seen more and more of these email attacks. You can tell users not to click on links or open attachments from senders they don’t know, but they’re only human. They are going to make mistakes from time to time, so you can’t rely on them as your only defense.

“All firms are exposed to a wide range of different attacks, making it is very hard to prepare for them all. The main impact of these targeted attacks has, to date, been on the IT department: “Every time something got through, we’d have to drop everything and deal with it. That would typically take up to ten people a couple of full days, during which time they are not doing the things that add value to the business.”

## Real-time URL Scanning

With BLM having relied on Mimecast Unified Email Management for email security - as well as archiving and continuity - since 2010, Darren immediately turned to Mimecast for an additional security layer. Specifically, he looked at Mimecast Targeted Threat Protection, which extends traditional gateway security to defend against malicious URLs and attachments in email – via its URL Protect and Attachment Protect services.

Darren initially set out to protect against URL-based threats, trialing and then rolling out URL Protect to help defend all of BLM’s 1,700 employees.

He said: “I had no hesitation in going with Mimecast Targeted Threat Protection. URL Protect is a really simple, smart way to cover a growing risk exposure in email, and deployment could not be easier. It was literally a few clicks in the administration console to protect the whole firm; it was a very, very easy way to roll out a mass solution.”

## **Attachment Sandbox**

Four months later, in November 2015, Darren added Attachment Protect to BLM's email security armory, again in response to heightened risk from weaponized Office and PDF attachments. Mimecast has significantly reduced BLM's risk of email security breaches via targeted threats.

Darren said: "The fact that Mimecast Targeted Threat Protection scans email in real-time and removes threats, either by rewriting URLs and scanning websites, or by sandboxing attachments, makes it a sure-fire solution. We can be confident that we are thoroughly protecting our employees against targeted attacks in email."

Prior to deploying URL protect, BLM was receiving hundreds of malicious email links via email every week – all are now scanned and blocked by URL Protect: "It's basically stopped that particular type of threat in its tracks. But it also helps us to target user education, by providing reports that tell us which users have tried to click on suspect links."

Attachment Protect scans and sandboxes around 37,000 attachments per week. Darren said: "Mimecast gives us the peace of mind that comes with knowing that any malicious attachments will never reach users. What's more, it's all but invisible to users, they don't even know that Attachment Protect is working in the background."