Case Study

mimecast

How United Synagogue Secured a Multi-Site, Hybrid Email Environment to Defend Vital Services and Secure Sensitive Data

Email archiving and security, along with simplified, centralised management across 65 sites, de-risked the organisation's hybrid M365 environment by securing against advanced email-borne attacks – to eliminate significant cyber risk and aide GDPR compliance.

The United Synagogue (US) is a union of British Orthodox Jewish synagogues, representing the central Orthodox movement in Judaism.

With 64 congregations and 60,000 members, it is the largest synagogue body in Europe and provides members with a diverse range of services – from creches and kindergartens to funeral and burial services.

The Synagogue also operates a commercial arm, whose activities include the supply of certified Kosher products and international Kosher inspection services.

At a Glance

- Supports 500 email users across 64 sites.
- The organisation was seeking to secure its hybrid M365 environment against advanced email threats including impersonation and malicious URLs.
- It needed improved data leak prevention capability as part of a wider GDPR compliance initiative.

Company

The United Synagogue (US) is a union of British Orthodox Jewish synagogues, representing the central Orthodox movement in Judaism. With 64 congregations and 60,000 members, it is the largest synagogue body in Europe.

Products

Perimeter Defence Plan (Secure Email Gateway & Target Threat Protection), Internal Email Protect, Continuity, Archiving, Sync and Recover and Secure Messaging.

Benefits

- Defends United Synagogue's email environment against advanced threats.
- Scans more than 220,000 emails every month, rejecting 61% of inbound messages.
- Sandboxes around 13,000 attachments, blocks more than 300 malware instances, and protects around 3,000 in-email URL clicks every month, while regularly detecting impersonation attacks.
- Secures sensitive date against human error and aides GDPR compliance.
- Internal email scanning, sync and recover ease incident containment and recovery.
- Saves support time and enables IT to focus more on higher value development work.

Given the scale of the United Synagogue's member network, the range of services it provides and the need to operate as a single consistent entity, communication across the organisation is vital – and over the years, email has become its primary communication tool.

IT Manager, Mark Shear, explained: "Email is one of the most important tools we have. All our sites need to communicate with each other, with head office and with members, while our food inspectors send back reports from all over the world. That means we need an email environment that is reliable, secure and, with a relatively small IT team, easy to manage."

Consolidating Legacy Systems

However, when Mark joined the United Synagogue, one of his first priorities was to overhaul an unstable, disparate email system, which combined an aging Exchange Server at head office, with a range of POP, IMAP and SMTP legacy systems across the organisation's 64 membership sites.

"The first priority was to put in place a secure archive, unified gateway security across the estate, and email continuity, before gradually migrating the whole organisation across to M365," he said.

"We chose Mimecast to provide all those requirements and de-risk our move to cloud email. It was the ideal solution, giving us a secure cloud archive, outstanding gateway security and easy to use continuity in the event our server went down. What's more, with centralised management, it saved us a lot of support and maintenance time."

Today, around 80% of United Synagogue's email environment has been migrated to M365, with the remainder soon to follow. "We got Mimecast in and never looked back," Mark said. "The archive makes sync and recover so easy and even retains our folder structures – and by integrating that with email security and continuity, Mimecast made us feel a lot more confident about moving forward with M365."

Emerging Threats, Human Error and GDPR

Of course, a move to M365 brings its own issues, not least the risk posed by new email-borne threats that M365 native security controls were struggling to contain.

"We were seeing lots of these advanced attacks. The main threats out there were fake URLs and impersonation attacks. We'd see an email from the old chief exec asking the finance director to make payments or click this link and we simply were not sufficiently protected against that kind of attack."

Mark was under no illusions about the risks posed by the United Synagogue's exposure to these advanced threats: "The big risks were system damage and data leaks. The reputational damage would be huge, and any data breach would inevitably affect our GDPR compliance, which was a big focus at the time."

Meanwhile, Mark's small team was stretched dealing with security issues reactively. "We were spending far too much time dealing with issues after the fact," he said. "We support 60 sites with a team of 9 including developers, so the support side is quite small, and it was getting to the point where firefighting was affecting our ability to deliver new services that support an enhanced experience for members."

Human error was also an issue Mark was wrestling with, despite regularly running user training around use of data and security. "We have a lot of volunteers working in the organisation, and sometimes the awareness around data privacy and use of email isn't what it should be" he explained.

"We didn't have very serious, significant incidents, but even putting an entire membership list in the 'to' field is a data protection issue and one we needed to be able to prevent rather than mop up."

The Ideal Solution

As an existing Mimecast customer, it was easy for United Synagogue to address these issues, quickly adding new features to prevent data leaks and defend against advanced, targeted email threats.

It was able to quickly deploy Mimecast Content Control and Data Leak Prevention to guard against the accidental or unencrypted sharing of sensitive information, like member lists and financial information,

Meanwhile, adding Mimecast Targeted Threat Protection to its email environment brought an additional layer of protection, particularly against malicious URLs, weaponised attachments, and impersonation attacks. Similarly, Mimecast Internal Email Protect was selected to help contain the spread of malware via email, within the organisation.

According to Mark, it was an easy decision with deployment backed by expert, responsive support: "Just to have these extra layers of protection, scanning URLs and attachments and flagging impersonation attacks, plus data leak prevention and internal email scanning was a no brainer.

"Anti-virus on individual machines is supposed to be the last line of defence, but you really don't want it to be – you want to stop it before, so nothing gets onto machines in the first place and that is exactly what these Mimecast solutions are designed to do.

Targeted Attacks Blocked

Mimecast Targeted Threat Protection has proved a highly effective solution, according to Mark:

"It's beautiful. I'm so happy with it. I used to have trouble sleeping for worry over email, the sheer scale and importance of it, from members to factories and food inspectors going all over the world. The worry was it would go down or be compromised."

"With Mimecast in place, that is a thing of the past. It keeps malicious URLs outside our environment, sandboxes suspicious attachments and stops impersonation attacks in their tracks. Now I can have a great night's sleep."

Mimecast scans around 220,000 emails each month, 30,000 of which are internally generated, rejecting around 61%. It blocks around 300 emails carrying malware every month, sandboxes 13,000 attachments, and protects around 3,000 in-email URL clicks, while regularly detecting and thwarting impersonation attacks.

"Getting it all rolled out and set up was so easy too. We had great support from Mimecast to help configure everything and then ongoing support to make sure we are getting the most we can from our investment. In fact, Mimecast, out of all our suppliers, is the best in terms of support. I call a local number and seconds later I am on the phone to an expert who can help there and then and knows the product inside out. There is no waiting for a call back."

Preventing Data Leaks

Similarly, Mimecast Content Control and Data Leak Prevention has helped to keep important data safe and secure, preventing accidental leaks.

"We did a lot of data leak prevention work, which Mimecast was a big part of," Mark explained. "That ranges from configuring policies to prevent member list details being shared in the 'to' field, to more sophisticated controls designed to prevent sensitive documents being accidentally attached to emails. We got a lot of help from Mimecast to set that up and it works very well."

Contain and Recover

On top of all that, Mark has the added peace of mind that comes with knowing that United Synagogue can quickly contain and recover from any attacks that do get inside the organisation, via email or any other route.

For instance, the Mimecast Archive provides seamless sync and recover features, allowing Mark to easily roll back to a safe backup, while Internal Email Protect ensures malware inside the organisation cannot spread via internal email.

Mark said: "I don't know of any other service that provides so many features in one place. Internal Email Protect is another line of defence, which ensures internal email goes through the same checks as external email."

"Quite recently, one of our machines was compromised and started sending out hundreds of emails. We were able to sit back and watch Mimecast rip it all out, removing 500 emails in an instant. Before we'd have been running around, making calls, to warn people not to open emails."

Flexible and Efficient

Putting additional layers of security in place has not only helped United Synagogue to protect its systems and data; it has also helped Mark's team to make more efficient use of time thanks to easy management and a more proactive security footing.

"That's the great thing about Mimecast," he said. "It sits in the cloud and everything has to go through it, so it is literally like a set of steel doors that nothing will get past unless you want it to. It's the gatekeeper and it's all very easy to manage."

"The Administration Console is great. It's such a comprehensive source of email insight, from message flows to threat intelligence, and saves so much time by enabling us to centrally manage security, archiving, policies and so much more. It's so flexible too; there are lots of options, so we have the ability to manage it how we want."

"There's no doubt that, without Mimecast keeping us on the front foot and mitigating risk, we'd be running around like headless chickens fixing machines, and that would take away from the development work that delivers new services and so on."

"Overall, I'm delighted. It's impossible to be 100% secure of course but having Mimecast in place is like putting your money in Fort Knox. I feel there is a huge weight behind the product and security-wise, it is fantastic."