# newlife
## THE CHARITY FOR DISABLED CHILDREN

**Company:** Newlife the Charity for Disabled Children

**Industry:** Not-for-profit

**Challenge:** Newlife, the UK's largest children's disability equipment charity, required robust security across all of its sites to protect employees from web, email and cloud based attacks and ensure high data governance.

**Solution:** Email Security, Email Archive, Sandboxing, Web Security, CASB, MFA

## Newlife sees cyber threats slashed to zero with Censornet

Newlife is the leading charity providing specialist disability equipment to disabled and terminally ill children across the UK, often in emergency crisis situations. The charity's work is funded largely by Newlife's unique commercial operation which takes donations from more than 240 retailers and manufacturers across the UK and Europe and sells them on in its network of seven stores. The items are unsold goods which are either end of line, surplus stock, customer returns or faulty and would otherwise be sent to landfill. It is a complex operation involving staff at multiple sites – a mix of offices, stores, warehouses, and homeworking – and more than over 150 staff and volunteers are working at any one time.

Unfortunately, Newlife had been targeted by cyber criminals looking to leverage funds and, as a not-for-profit organisation, it must also ensure it has the highest level of governance to protect its staff, donors and the families being supported by the charity.

Phil Ashcroft, Technology Manager at Newlife, explained: "It may come as a surprise to readers that we face more attacks on the charitable side of the organisation than on the commercial side. Unfortunately, charities are a major target for hackers. Accordingly, we have to be extremely vigilant in ensuring we are protecting our data and our traffic, and mindful our security could, rightly, be audited at any time by The Charity Commission, so it is vital we have clear, easily documented protection in place."

## Protecting employees and volunteers over the web and in cloud applications

Newlife procured Censornet's web and cloud security solutions in November 2017. With Censornet, Newlife has gained insight into the web traffic coming from its network and is able to apply rules and restrictions to protect users and stakeholders from any dangerous sites online and protect sensitive donor data.

> "Censornet ticked all of the boxes. It integrated seamlessly with our Office 365 environment and because it is based in the cloud we have visibility and control from one pane of glass across all of our sites"
>
> **Phil Ashcroft, Technology Manager at Newlife**

**censornet.com**

# censornet.

Censornet's cloud access security broker (CASB) also means that Newlife can control the applications employees access. For example, limiting staff to their Office 365 accounts and applications and blocking personal applications that could put the charity at risk.

Phil added: "In-built permissions over what our staff can and can't access improves productivity and security. The risk from the web is well known but without the addition of cloud security, there is a risk staff could be downloading dangerous files from applications without even realising it. Overall, the control from Censornet, and the ability to drill down into traffic coming from the web and cloud, gives us greater security that we aren't going to be hacked."

## Protecting employees and volunteers on email

In November 2019, Newlife added Censornet email security to its arsenal to help protect against the most common attacks it was facing - phishing and impersonation attacks over email. While the charity had advanced threat protection provided by Office 365, it was still experiencing between 20 and 50 threats a day over email. Impersonation attacks against the CEO and the finance team were particularly common and a concern.

"It became obvious to us that the email security provided by Office 365 wasn't giving us adequate protection and it needed to be enhanced," added Phil. "We experienced several attacks a day over email, often impersonating members of staff, and it began to damage the productivity of the charity as staff struggled to tell if an email was legitimate or not."

Censornet has reduced the number of email threats the organisation faces from between 20-50 a day to zero. One of the major benefits for Newlife is that their employees can now trust that the charity is protecting them so they don't have to worry as much about keeping safe online, in applications or on email.

"We even tried to beat the Censornet system ourselves," Phil admitted, "but the system is too intelligent, no threats get through. This means our staff are now assured that any emails they receive are legitimate and they are better able to effectively carry out their jobs. We have received brilliant feedback from staff on the Censornet products, especially LinkScan, which allows them to scan emails for threats.

"This also has a knock on benefit for the IT team, as we used to be inundated with calls for employees about suspicious emails and links. Now we have more time to go about our jobs. Security education is obviously important but Censornet has shown us that that the ideal situation is assurance that staff are secure by default."

"In-built permissions over what our staff can and can't access improves productivity and security. The risk from the web is well known but without the addition of cloud security, there is a risk staff could be downloading dangerous files from applications without even realising it."

**Phil Ashcroft, Technology Manager at Newlife**

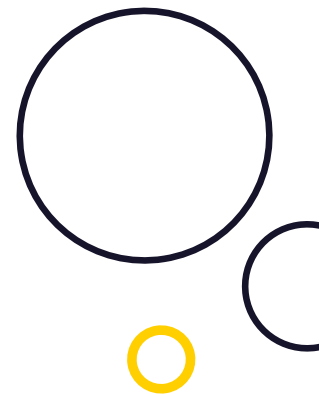censornet.com

**censornet.**

## Security that combines people and technology

Both the technology and the team behind Censornet were major factors for Newlife when choosing a security solution for web, cloud and email.

It was important to the charity that all of the solutions were cloud based so that the IT team could protect their staff consistently across their 14 UK sites. Censornet's platform also means that the tech team don't need to access different portals to administer products, they have a single overview of email, cloud and web and can drill down and analyse any vulnerability they see across any prod-uct. The intelligence of the Censornet product also means that, where the charity used to have to run reports and cross reference threats across different platforms, threats will now automatically be flagged across email, web and cloud if flagged in one of the products.

Phil explained; "The first consideration when choosing a security provider is the quality of the product, and Censornet ticked all of the boxes. It integrated seamlessly with our Office 365 environment and because it is based in the cloud we have visibility and control from one pane of glass across all of our sites. There's no messing around with different portals or VPNs to change security responsibilities, we can just go online and make changes which takes a massive strain off of us."

"However, there is also a second, more human element to choosing a security solution - you also need to make sure that you can work with the people and get the support you need. This is where Censornet has excelled, through the onboarding and implementation process and beyond. They made their CTO available to us, which not many companies do, and the expertise and knowledge at Censornet is world class. There is never any red tape we need to go through, they are just a phone call away, which is extremely important and valuable for an organisation of our size. The support has been the biggest win for me be-cause the last thing you want in security is additional complexity, especially in a crisis situation."

**censornet**