SOPHOS

PARTNER CASE STUDY

newfox
passionate about making IT happen

Partner-at-a-Glance

Newfox
Newfox are a Yorkshire based technology solutions and support provider.

Client Industry
Social care

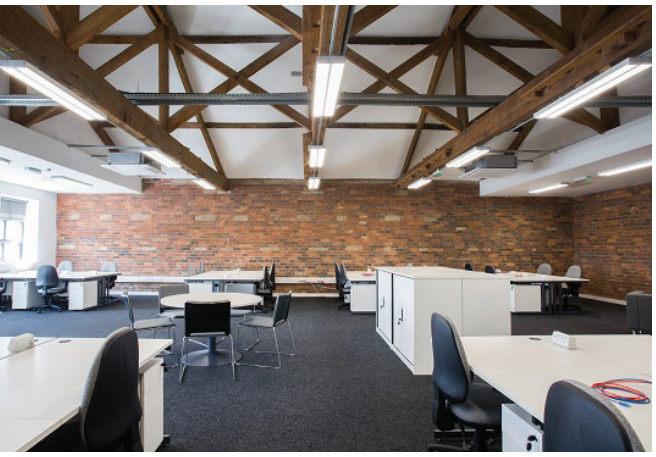
Number of Staff
100

Sophos Solutions
Sophos Central Mobile
Intercept X

Sophos Partner
Since 2017

Newfox and Sophos instrumental in uncovering location of SamSam ransomware attackers

Leeds-based Newfox provides end-to-end IT solutions, including IT security, helping hundreds of businesses to keep systems and data safe. Here we find out how their quick thinking helped protect a leading manufacturer of medical technology equipment while also working with Sophos and various law enforcement agencies to track down the Iran-based attackers.



'The Iranian defendants allegedly used hacking and malware to cause more than $30 million in losses to more than 200 victims. The criminal activity harmed state agencies, city governments, hospitals, and countless innocent victims.'

Former Deputy Attorney General Rod Rosenstein, the United States Department of Justice

In the autumn of 2018, the team at Newfox were migrating the server estate of its customer, a medical technology manufacturer, also based in Leeds. The ransomware protection the company had in place needed to be temporarily and partly removed in order to migrate the estate, yet during this time a ransomware attack named SamSam took place.

The ransomware attack

The ransomware used in this attack tried to move sideways across the entire estate in an attempt to lock down the company's files. It was unable to do so because Intercept X from Sophos was still present across many areas of the network. Instead, it was only able to leave its payload (the component of a computer virus that executes a malicious activity) and the detonation key, which gave Newfox the beginnings of an idea about where it might have originated from. The exploit hadn't been able to run, but it had left some clues along the way.

Meanwhile, the SophosLabs team had identified that an attack had taken place. Sophos Central, an award-winning security console installed at the medical technology manufacturer, alerted the SophosLabs team that a serious incident had been detected through Intercept X.

Tracking the attackers

Newfox located the payloads and handed them to SophosLabs, where urgent work began to reverse engineer the code and fix any damage left behind by the encryption payload. This was a lengthy process but one they hoped would enable them to track down the SamSam creators, who had received $6 million in reported ransom payments and caused over $30 million in losses, including shutting down the entire government infrastructure of Atlanta, Georgia. Newfox also worked tirelessly to remedy the situation for its customer, which they managed to do quickly and efficiently without impacting business continuity.

After many hours of detective work, Newfox and Sophos were able to submit their findings to the West Yorkshire cybercrime unit, which alerted the U.K. National Crime Agency. The FBI then became involved. The attackers were rapidly identified and subsequently indicted in their absence as they were located in Iran.

Always Sophos

Newfox will now only ever recommend Sophos products to its customers. "We know it works first hand and we have seen it solve a large-scale international crime," says Craig Owens, managing director at Newfox. "As a result, we are incredibly confident in Sophos and now only ever recommend their solutions to our customers."

In turn, Sophos helps Craig to grow his company through training his staff all the way to Sophos Architect status and keeping the company abreast of the latest threat updates.

International crime fighting

The quick thinking and the actions carried out by Newfox and Sophos meant that the two high-profile criminals behind the SamSam ransomware virus are now identified and have had their activities curtailed following a 34-month-long international computer hacking and extortion scheme.

The medical technology equipment manufacturer has returned to business as usual without any interruption to its work, and the close relationship between Sophos and Newfox IT continues to provide trusted products and expertise in the fight against online crime.

To find out more about Newfox and how they can help protect your business, call 0113 887 4311 or email info@newfox.it.

'We manually found the attackers' buried code using Intercept X from Sophos, and this helped to track them down.'

Craig Owens
Managing Director, Newfox

'We were able to rebuild the entire server estate in just a few days. With no downtime to the client, our team was relentless in ensuring everything was back on track for our customer. We also received brilliant guidance from Sophos.'

Phil Drew
Sophos Architect, Newfox

To find out more about Sophos solutions,

call (0)8447 671131 or email sales@sophos.com.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-07-01-CSNA (NP)

SOPHOS