RelianceCyber

DELT SHARED SERVICES

Reliance Cyber & DELT

ANALYSIS, PREDICTION, ACTION

Next-level cyber security for NHS, GPs and local government

reliancecyber.com

AT A GLANCE

The Challenge

In the wake of multiple NHS and local government cyber incidents and data privacy issues, shared services specialist Delt needed to transition its customers – including 160 GP locations - away from a reactive, security software-only mindset to 'always on' monitoring, expert human threat insight, and predictive action.

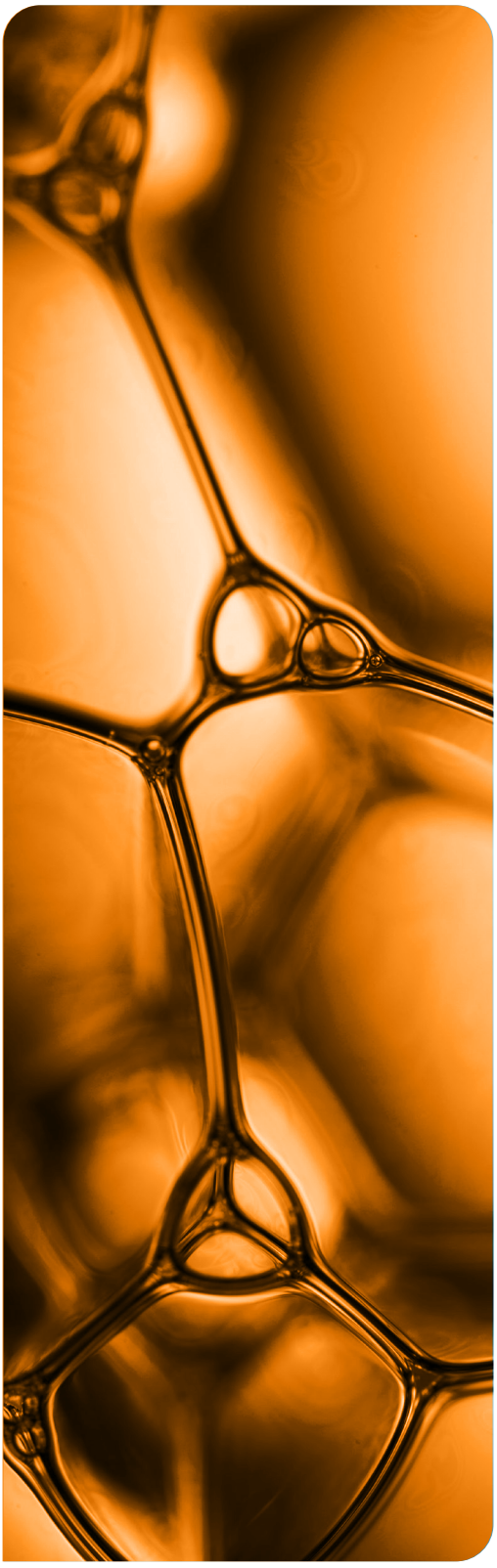
The Solution

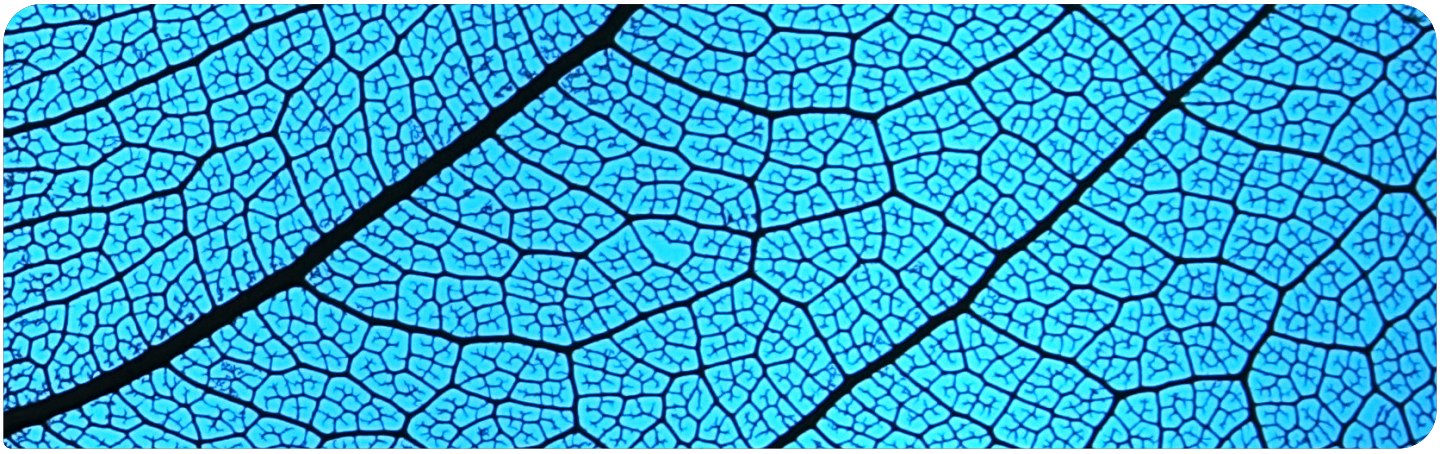
Delt chose 24x7x365, Extended Detection and Response (XDR) services from Reliance Cyber, who delivered "by far the best engagement of all the providers."

The Result

"The XDR services Reliance Cyber deliver have reduced our exposure, and that of our local government, NHS and GP practices, significantly."

Giles Letheren, CEO, Delt



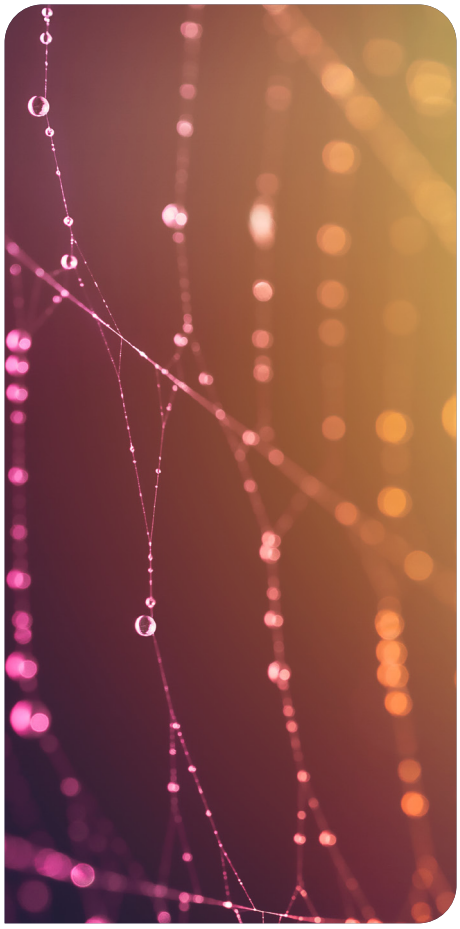


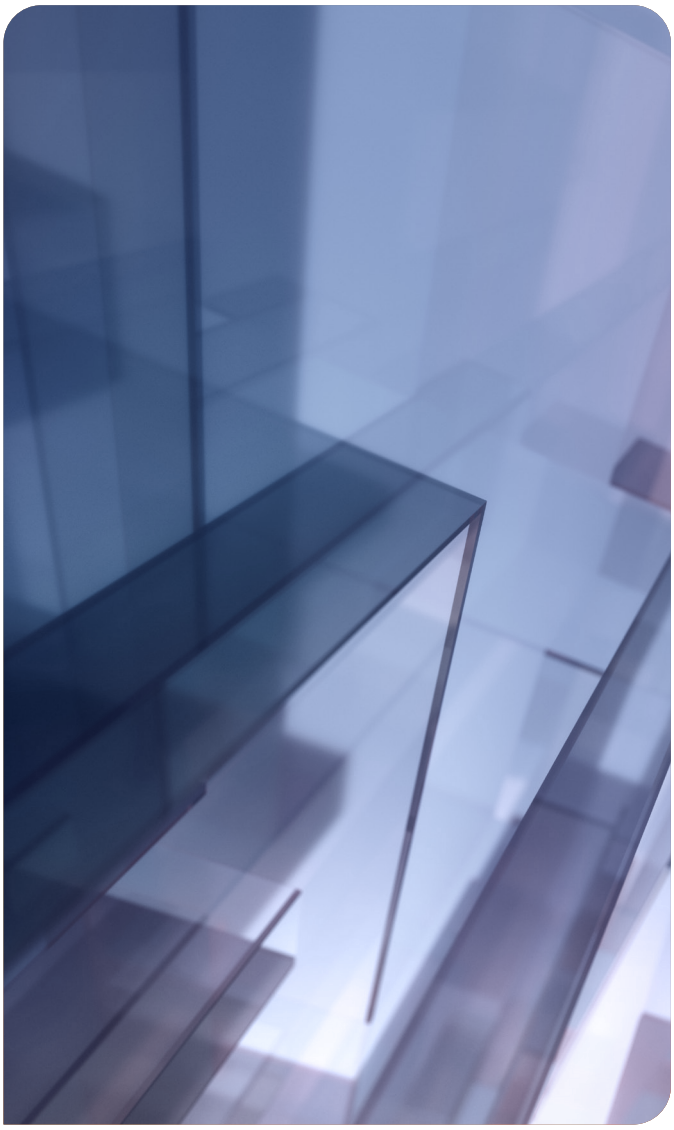
The Challenge

Shared services specialist Delt (www.deltservices.com) delivers a wide range of key services, including IT, Payroll, HR and Print Services, to a rapidly growing portfolio of public sector customers in the South West, including NHS England, the regional Clinical Commissioning Group, Plymouth and Torbay Councils, Plym Academy Trust, and many other vital healthcare, education and community entities.

But with recent incidents bringing these organisations' cyber security under more intense scrutiny from central Government than ever before, reactive strategies based around security software had been exposed as ineffective.

To deliver security that was fit for purpose, Delt needed to be able to constantly monitor its customers' networks, analyse evolving data, and use this to counter threats predictively.





This produced a number of challenges.

With a growing customer base, Delt needed to deploy security rapidly across the complexities of multiple sites with highly differentiated requirements (every GP practice, for example, is essentially an independent business, with its own operational processes and procedures).

They needed to change users' behaviours as frictionlessly as possible, so that they learnt to act securely by default.

And they needed to demonstrate real value for money and ROI against the additional Government cyber security funding that had been made available in the wake of the WannaCry attack.

On all counts – and more – Reliance Cyber delivered.

The Solution

Giles Letheren, Delt's CEO, is clear that for a new era of threats, a new kind of security solution – and a new way of evaluating the companies that provide it – was necessary.

Historically, he says, public sector IT strategy was up against ever-dwindling budgets, so organisations went for the cheapest security stance possible: deploying reactive software that would supposedly do the job for them and enable them - on paper – to put a tick in the compliance box.

But this over-reliance on technology meant there were few – if any – internal customer experts who understood IT security issues and could impart security knowledge and awareness across the organisation.

Further, WannaCry and a whole raft of other cyber incidents had already demonstrated that the reactive mindset that security software encourages is not an effective defence against today's threats in any event.

"What we needed," confides Letheren, "was a totally different security model. We were looking for a provider who would use both technology and human expertise to monitor and make constant sense of each customer's ongoing security posture and the threats ranged against it, predict what was likely to happen next, and then produce clear and flexible action plan options."

He continues: "A lot of security service providers promise this but what they actually deliver is 'one size fits all' templated reports that are unhelpful."

"So we decided to actually test providers in situ, not only to see how effective their security proposition was, but how closely they engaged with us on security matters day to day."

A shortlist of security service providers was drawn up, including Reliance Cyber, and each provider was asked to deploy a pilot across three sites – one small, one medium and one large.

"Effectively," says Letheren, "we turned the normal tender process on its head to cut through the hype and test what the security providers could really deliver."

After just one month, the outcome was unequivocal - Reliance Cyber and its Extended Detection and Response (XDR) service outperformed all the other providers.

XDR

What it is and what it delivers

Extended Detection and Response (XDR) combines multi-vendor security technology, artificial intelligence and human analysis to monitor customers' networks 24x7x365, and to proactively hunt out and shut down even unknown and potential threats that could target organisations' specific asset risks (confidential patient data that can be used to create false identities in the case of a GP practice, for instance).

In this way, XDR's defensive resources – both technological and human - are always focused strongest where they will prevent the most damaging consequences for that particular organisation.

RESULTS AND BENEFITS

Bringing peace of mind

Letheren acknowledges that Reliance Cyber's range of security technologies delivered in a Managed Security Service Provider (MSSP) arrangement from the cloud, have proven highly effective, available and economical - but he's also quick to point out the strategic and collaborative value of Reliance Cyber's people, too.

"They had by far the best engagement of all the providers," he says. "They worked with us in a far more collaborative way than the others."

"Their core business is human cyber threat insight, so their analysts take the time and trouble to understand the customers and their operating risks in a personalised way most other security providers don't."

"Their outputs deliver more value, too. The security data and analysis they produce, for example, quite clearly comes from human experts with a knowledge of that customers' security needs and priorities, not from standardised templates."

"And importantly, when it comes to taking action, they always ask 'Do the actions we're recommending here work for you and your customers, and if not, what would work better?'"

Letheren says that Reliance Cyber's approach to security as a journey – not a destination – makes for a more holistic offering that can deliver real long-term cultural change, too.

"The Reliance Cyber experts actually came into Delt's offices and worked directly with our teams to help customers adopt secure behaviours with minimum effort and impact on their daily routine. They leave a real, lasting legacy of user security awareness that is a critical layer of defence in any organisation."

But ultimately, the effectiveness of a security strategy is measured by whether or not it clearly diminishes the overall risk of a cyber incident – and on this point, Letheren is unambiguous.

"The XDR services Reliance Cyber deliver have reduced our exposure, and that of our local government and NHS organisations, and GP practices, significantly," he asserts.

Powerful medicine indeed.

RelianceCyber

Get in touch

+44 (0)845 519 2946
contact@reliancecyber.com

reliancecyber.com

DELT LTD
SHARED SERVICES