How CLTD Secured Its Hybrid Workforce Without Disrupting the Way People Work

At a glance

Challenges

- Keeping critical data secure everywhere
- Integration into existing systems
- A system that would work for all staff

Results

- User-friendly systems and strong protection
- Fall in detected threats
- Reduced Board reporting time

No Time To Lose: The Challenge

'"I had nights when I'd stare at the ceiling and wonder if a hacker had got into our systems,' says James DeLarn, Operations Director at CLTD.

Remote work has become the 'new normal', but with that comes 'new concerns' about keeping systems and data safe as staff work from home.

"Our workforce was now working from home in the UK and Europe, using company and personal devices," DeLarn explains.

"Offering work-from-home has allowed us to attract the best people for our company as it has become a valuable benefit."

However, hybrid working also creates significant security challenges.

A larger attack surface

When the company started WFH (Work From Home), its security team noticed an increase in phishing emails and social engineering attempts.

"It's like having several small offices in different countries, all with their own security needs," DeLarn says.

The company wanted a specialised approach, so their hybrid security would integrate seamlessly with their existing security systems.

They chose RT Security because it had experience handling this type of situation.

Integrating new security into existing systems

> "*We were concerned we'd have a complex security system that staff would find difficult to use.*"

Martin Davies, RT Security's Director of Customer Installations, explains that "we did a thorough assessment of CLTD's existing infrastructure and what would work for both staff and the company.

Once we'd finished our assessment, we sat down with James and staff from different departments to create a security strategy that works for everyone."

Davies goes on to say: "This is important. If systems and procedures are overly complicated, staff will avoid using them or find their own solutions.

In both cases, this can create gaps in a company's security posture, which is the last thing you want.

Our role was to balance keeping the systems as secure as possible, installing new hybrid security and making it all as user-friendly as possible."

Multiple security measures

Staff use several devices and often travel to the office with them. RT installed a new system, giving them 'endpoint protection'.

Now, every device connecting to the company's system is secure, and new rules are also in place to prevent unauthorised access to sensitive data.

A more powerful Virtual Private Network (VPN) encrypts traffic moving over the network and allows staff to access company data securely.

Staff now use passwordless authentication, which has proved popular because they no longer have to remember lots of different passwords as they did before.

In turn, this has strengthened security across the company.

Customised training makes security easier to learn

RT also created customised training that met the specific needs of different staff members, so everyone learned practical ways to protect their devices and data.

This was a change from our usual one-training-for-everyone approach, DeLarn explains.

"We'd never used customised security training before, and it was a success. Staff found it easy to follow, and several commented that it was practical and much more user-friendly than they expected.

Added to this, several staff have since spotted and reported unusual activity."

Another problem RT helped solve was reports for Boards and stakeholders.

Delivering even more value

As Martin explains: "Our clients often have to report to their Board, so we provide them with the facts and data they need, in an easy-to-understand format, with a business focus.

This way, they can explain to stakeholders, shareholders and suppliers how the new security systems benefit the company and keep them up-to-date going forward."

> *An unexpected benefit: increased productivity.*

The Results Are In

DeLarn says, "Detected threats have dropped, staff feel more confident to report anything suspicious as the new reporting system is much easier to use.

And then there was another unexpected benefit, increased productivity.

"We found that staff were waiting to come into the office if they needed to access sensitive information.

With the new security in place and having taken the training, they felt confident accessing data away from the office."

RT kept downtime to a minimum and worked with the company's other security suppliers to ensure all the systems worked smoothly together.

DeLarn says, "With RT's solutions in place, I sleep better knowing that our data and systems are secure.

Now, our staff can work in a way that's right for them and means we can attract and keep talented people, helping our company to thrive."

At a glance - the results

- Drop in detected threats
- Increased staff confidence in reporting
- Unexpected productivity boost
- Reduced Board reporting time