daisy. CORPORATE SERVICES
Part of the Wavenet Group

Support & Managed Services

Cyber Security

CUSTOMER PROFILE

CLOUD-BASED SECURITY SOLUTION ENABLES SECURE AND ROBUST NATIONAL VACCINE ROLL-OUT.

The customer, a government agency in England, is responsible for the protection of public health and infectious disease capability, as well as the planning and execution of the response to external health threats. With a headquarters based in London, England, it employees between 1,001-5,000 employees.

AT A GLANCE

Industry sector: Health

Employees: 1,001 - 5,000

Solutions/services taken:

- Managed Services
- Cyber Security

Total Contract Value: £120K per annum

Length of Relationship: >10 years

The Business Challenge

Having been a Daisy customer for more than 10 years, and with 11 servers hosted in Daisy's Flex service, the customer was operating and utilising an Immform application; a system that allows the recording of data in relation to uptake against immunisation programmes and incidence of flu-like illnesses, as well as allowing for all UK-wide medical practices and surgeries to order vaccinations required for any specific programmes or to fulfil local need/requirement.

With a national threat risk being posed at the time by the emergence of a new coronavirus and with countries across the globe scrambling to get the pandemic under control, further complications arose in terms of which country would be the first to develop an effective vaccine and subsequent robust vaccination programmes. This meant the customer faced a much higher-than-normal risk of politically-motivated cyber attacks on the data it held in its servers. Therefore, the integrity and security of the data held and handled by the customer – as well as every British citizen - was paramount.

Further to that, as and when any vaccination was tested and delivered, the distribution of said vaccine programme would also face potential issues due to red tape caused by Brexit and the logistics of moving goods both in and out of the country.

Due to such levels of associated risk, an audit of what was already being delivered to the customer was carried out which subsequently identified a number of potential security enhancements that would be required and at this time. In addition, Daisy's cloud consultants recognised the potential to improve the service being provided to the customer which would include a series of upgrades and updates.

The Solution

Daisy's proposal included a cloud-based security wrap around the existing solution being provided which included DDoS and a SIEM that would proactively identify any vulnerabilities.

Daisy's DDoS Protection service (DDP) - network-based service, would provide the customer with Daisy Internet connections and Internet-facing hosts, with mitigation against the threat of DDoS attacks. During an attack, the customer's traffic would be redirected through Daisy's DDoS mitigation platform which either blocks all traffic or intelligently identifies and drops malicious attack traffic. This all happens within Daisy's core network before it reaches the customer's port where it will cause the most damage.

The SIEM solution would allow the customer a centralised view of the entire environment. This is important because more visibility means the solution is more effective at identifying risks. The SIEM platform would also monitor the environment for indications of potential vulnerabilities or active compromises. Should the SIEM platform detect anything which requires investigation, this will be alerted to the Daisy Security Operations Centre (SOC) team. The SOC team will triage the alert and make a recommendation as to the required action.

The Results

The turnaround time of the upgrade project was just three months with a total contract value of £120K per annum. During project roll-out, the customer didn't experience any security breaches that impacted service, and as a result, the UK's vaccine programme was successfully rolled out; a huge achievement in the face of a major global pandemic.

In addition, because the solution is cloud-based, from an environmental perspective, it also allows the customer to operate core capabilities with a reduced carbon footpris the case with many higher education institutions, ESG is always a consideration and with the introduction of the all-flash storage arrays, the customer was able to benefit from substantial power and cooling savings which would go some way to reducing its carbon footprint.