Case Study

sense

Removing complex IT with a Managed Secure SD-WAN

About Sense

Sense is a leading UK charity which helps those who are living with complex disabilities, or are deaf blind, to communicate and experience the world. As well as providing practical support, the charity champions the rights of people living with complex disabilities, at a local and national level, and has experienced many landmark moments over the years, campaigning to change laws and government policies.

Founded in 1955, Sense has gone from an organisation with assets of two pounds and five shillings (£48 in today's money), to an annual turnover of over £60 million. It has 10 branches around the country and trades through 109 shops. Sense is also a membership organisation, with almost 4,900 members, and, according to its latest Annual Report, employs.

Business challenge

Sense conducted a strategic review of its connectivity and computing capacities, and as a result asked TITANIUM approved Managed Services Provider, TIEVA, to recommend alternative solutions capable of meeting its current and future operational needs.

The organisation was operating the majority of its critical business systems from physical server hardware, co-located within a third-party data centre. This hardware was reaching the end of its useful lifespan and its lack of capacity was constraining both system performance and Sense's ability to adapt to changing demands.

To compound the operational issues, for historical reasons, Sense's operating locations were connected to the outside world via two different line providers. This lack of cohesion generated both operational and performance bottlenecks, as user data and traffic travelled between the different networks.

This fragmentation of connectivity was also leading to data security challenges, as there was no logical perimeter to secure.

As a result of these challenges, alternative technology solutions were needed to secure the longevity of the organisation, decrease management overheads and increase the resilience, security and performance of application delivery throughout the organisation.

multiple geographically diverse data centre locations. This provided Sense with multi-layered protection against advanced cyber threats and visibility of the organisation's security landscape across its entire estate. For longer-term data retention, TITANIUM also deployed a back-up as a service (BaaS) solution, using technology from Acronis, to allow data from any source to be reliably and securely stored on a simple consumption-only basis.

The outcome

As a consequence of TITANIUM being deployed for Sense, the organisation has gained a stable and high-performing platform from which it can deliver the critical applications it needs.

This platform is augmented by an ongoing partnership between the technical teams within Sense and TIEVA, enabling Sense to access support from both TIEVA and TITANIUM's enterprise-level architects for ongoing change management and guidance, as well as reducing reliance on internal resources.

Having chosen to partner with TIEVA to implement TITANIUM, Sense has also been able to use the combination of technical expertise and technology provided to enable its own technical team to refocus its efforts from issue resolutions and instead concentrate on driving strategic changes for its operation. This will ultimately help to maximise revenue streams and enhance client care.

The solution. TITANIUM

To meet these challenges, TIEVA designed and implemented a comprehensive solution with TITANIUM at it's core.

A business-grade connection was deployed for all the organisation's sites, terminating on Fortinet SD-WAN hardware, to securely bring all site traffic back to TITANIUM data centres. This SD-WAN overlay allowed business-critical applications to be dynamically prioritised.

To provide an infrastructure as a service (IaaS) solution, TITANIUM created a virtual private cloud (VPC) with sufficient capacity to cover all of Sense's business applications, including its customer relationship management (CRM) and finance platforms. To ensure maximum availability of the IaaS solution, all resources within the VPC were replicated between two data centre locations, and, for the ease of financial planning, were provided on a managed, not metered, basis.

Perimeter security for the IaaS platform and the site connectivity was provided, as a firewall as a service (FWaaS) solution, using Fortinet next-generationfirewall (NGFW) technology, spanning