Trending: Security As A Service

Article By:

Cameron Abbott

Remember the time when you first heard about cloud computing and it took you a few moments of quiet contemplation before you wrapped your head around the concept of computing being situated "up there"? Of course today we aren't surprised to learn that over 80% of enterprise workloads will be in the cloud by next year and that a new wave of cloud-based security as a service (**SECaaS**) solutions are rolling in to address the forecasted USD $5.2 trillion per year in cybercrime damage that is expected to impact within the next 5 years.

Based on the software as a service (**SaaS**) model, SECaaS is a cloud-based managed security service that removes the need for businesses to buy and continually upgrade on-premises hardware and software and keep staff upskilled in the ever-shifting world of cybersecurity risk and protection.

For most businesses, SECaaS offers significantly more cybersecurity expertise than they would otherwise have access to and allows them to get on with their core business without being distracted by changing cybersecurity conditions. In practice, we're seeing businesses using SECaaS to manage email security (e.g. phishing and spam protection), user authentication and access, network security, vulnerability scanning, data loss prevention and disaster recovery.

While the idea of pushing cybersecurity woes to a SECaaS vendor is seductive, unsurprisingly businesses aren't able to have their cake and eat it too. There are still opportunities for interception by hackers at the send/receive connection points which means that businesses still need to be vigilant about security on-premises. Compounding the issue are staff who are exploiting one of the benefits of cloud computing – working remotely and on their own devices – which can limit the sphere of control a business has over its security. These risks would be present with or without SECaaS, however it shows that SECaaS is not a silver bullet when it comes to protecting businesses against cybercrime.

Despite this, it is forecasted that over 70% of businesses will be using SECaaS by 2021, indicating that having a continually monitored and updated SECaaS environment still outweighs SECaaS' limitations.

Co-Authored by Karla Hodgson

National Law Review, Volume IX, Number 220

Source URL:https://natlawreview.com/article/trending-security-service